# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-195269

(43)Date of publication of application : 21.07.1999

(51)Int.Cl. G11B 20/10

G09C 1/00

G09C 1/00

H04L 9/16

// G06F 17/60

(21)Application number : 09-369395

(22)Date of filing : 26.12.1997

(71)Applicant : VICTOR CO OF JAPAN LTD

(72)Inventor : HIRATA ATSUMI

MACHIDA TOYOTAKA

HIROTA AKIRA

(54) INFORMATION CIPHERING METHOD, INFORMATION DECIPHERING METHOD, INFORMATION CIPHERING DEVICE, INFORMATION DECIPHERING DEVICE AND INFORMATION RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an information ciphering method by

which a ciphering and a deciphering are relatively simply and inexpensively enabled and the estimation of a deciphering key is made difficult.
SOLUTION: An information control means 1 accumulates information key codes peculiar to digital information and information signals. A customer control means 5 accumulates customer peculiar certifying keys and reproducing device peculiar distribution keys. Then, a code conversion means 9a converts the information key codes and generates work key codes. An information ciphering means 11a generates ciphering key codes from the work key codes and the sector numbers outputted from the means 9a. Then, the sectored digital information data are ciphered by using the ciphered key codes.

---

LEGAL STATUS

| | |
|---|---|
| [Date of request for examination] | 29.09.2003 |
| [Date of sending the examiner's decision of rejection] | 14.11.2006 |
| [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration] | |
| [Date of final disposal for application] | |
| [Patent number] | |
| [Date of registration] | |
| [Number of appeal against examiner's decision of rejection] | |
| [Date of requesting appeal against examiner's decision of rejection] | |
| [Date of extinction of right] | |

## CLAIMS

[Claim(s)]

[Claim 1] In the information encryption approach which enciphers said digital information data in case it records on an information record medium with the sector number which divides digital information data into two or more sectors, and shows the rank of a sector Carry out code conversion of the information key code of a proper to said digital information, and a work-piece key code is generated. The information encryption approach characterized by enciphering said digital information data which generated the encryption key code from this work-piece key code and said sector number, and were sector-ized using this encryption key code.

[Claim 2] In the information decode approach which decodes said digital information data of the record medium with which the digital information data which were divided into two or more sectors and enciphered are recorded with the sector number which shows the rank of a sector The information key code of a proper is decoded to said enciphered digital information which is supplied from other than said record medium. Carry out code conversion of this information key code, generate a work-piece key code, and a decryption key code is generated from this work-piece key code and said sector number currently recorded on said record medium. The information decode approach characterized by decoding the enciphered digital information which reproduces said record medium and is acquired using this decryption key code.

[Claim 3] Said work-piece key code is divided into two or more partial bit string of the numbers of bits [ code / information key ]. After carrying out exclusive logical addition of the one partial bit string of the arbitration chosen from this partial bit string to each of other partial bit string, respectively, combine it and the first bit string is generated. Carry out exclusive logical addition of said information key code and the second bit string of the same number of bits to said first bit string,

and the third bit string is generated. After dividing into two or more partial bit strings of the numbers of bits [ bit string / said / third ] and carrying out low TETO only of the predetermined number of bits within each of this partial bit string on the right or the left, The information encryption approach according to claim 1 characterized by generating the fourth bit string unitedly, dividing said fourth bit string into two or more partial bit strings, changing the array sequence of each partial bit string, and being generated, or the information decode approach according to claim 2.

[Claim 4] Said encryption key code or said decryption key code is the information encryption approach according to claim 1 characterized by being the pseudo-random code train generated using the value just because it did the division of said work-piece key code with said sector number, or the information decode approach according to claim 2.

[Claim 5] In the information encryption equipment which enciphers said digital information data in case it records on an information record medium with the sector number which divides digital information data into two or more sectors, and shows the rank of a sector The code-conversion means which carries out code conversion of the information key code of a proper to said digital information, and carries out raw [ of the work-piece key code ], Information encryption equipment characterized by having an information encryption means to encipher said digital information data which generated the encryption key code from the work-piece key code outputted from this code-conversion means, and said sector number, and were sector-ized using this encryption key code.

[Claim 6] In the information decode equipment which decodes said digital information data of the record medium with which the digital information data which were divided into two or more sectors and enciphered are recorded with the sector number which shows the rank of a sector A key decode means to decode the information key code of a proper to said enciphered digital information which is supplied from other than said record medium, A code-conversion means to carry out code conversion of the information key code

decoded with this key decode means, and to generate a work-piece key code, A decryption key code is generated from the work-piece key code generated with this code-conversion means, and said sector number currently recorded on said record medium. Information decode equipment characterized by having an information decryption means to decode the enciphered digital information which reproduces said record medium and is acquired using this decryption key code.

[Claim 7] Said code-conversion means is divided into two or more partial bit string of the numbers of bits [ code / information key ]. A bit string division / addition means to combine it and to generate the first bit string after carrying out exclusive logical addition of the one partial bit string of the arbitration chosen from this partial bit string to each of other partial bit string, respectively, An addition means to carry out exclusive logical addition of said information key code and the second bit string of the same number of bits to said first bit string, and to generate the third bit string, A bit rotation means to generate the fourth bit string unitedly after dividing into two or more partial bit strings of the numbers of bits [ bit string / said / third ] and carrying out low TETO only of the predetermined number of bits within each of this partial bit string on the right or the left, said fourth bit string -- two or more partial bit strings -- dividing -- the array sequence of each partial bit string -- changing -- work-piece key code **** -- the information encryption equipment according to claim 5 characterized by things, or information decode equipment according to claim 6.

[Claim 8] Said encryption key code or said decryption key code is the information encryption equipment according to claim 5 characterized by being the pseudo-random code train generated using the value just because it did the division of said work-piece key code with said sector number, or information decode equipment according to claim 6.

[Claim 9] It is the information record medium characterized by for the digital information data divided into two or more sectors being the information record medium currently recorded with the sector number which shows the rank of a sector, and enciphering said digital information data using the encryption key

code generated from the work-piece key code which carried out code conversion of the information key code of a proper to said digital information, and said sector number.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the informational encryption/decode approach, and especially, when sector-izing information, such as a video signal, a sound signal, and a data signal, and performing record/playback to information record media, such as a disk, it is used, and it relates to the suitable information encryption approach, the information decode approach, information encryption equipment, information decode equipment, and an information record medium.

[0002]

[Description of the Prior Art] The decode key (or information corresponding to a decode key) for decoding the enciphered information is recorded on the same record medium at the same time it enciphers information using a predetermined encryption key and records on a predetermined record medium conventionally, when enciphering and recording information on a predetermined record medium. In this case, the decode key (or information corresponding to a decode key) is distributed and recorded on record or two or more not continuous fields succeeding the field where predetermined [ of a record medium ] continued.

[0003] Decode had decoded the enciphered information which is reproduced from the same record medium using the decode key which was reproduced and was obtained from the record medium, or the decode key generated based on the information corresponding to a decode key.

[0004] Moreover, encryption is enciphered using one cryptographic key about at least one information. For example, when the information on merit's film was enciphered for 60 minutes, the whole volume was covered for 60 minutes and it had enciphered using the same cryptographic key.

[0005]

[Problem(s) to be Solved by the Invention] Since the decode key (or information corresponding to a decode key) used in order to decode the enciphered information and its enciphered information is recorded on the same record medium, and covered the one whole information and had enciphered conventionally using the same cryptographic key, the technical problem that it was easy to presume a decode key occurred. Moreover, since the decode key (or information corresponding to a decode key) was recorded in the information record medium, the field for it needed to be secured in the information record medium, and the part and the fields which record original information were decreasing in number.

[0006] In addition, there is a PN addition method by the common key system as the comparatively easy and effective encryption/decryption approach. This method is also called a pseudo-random addition method, and enciphers information using an M sequence coder. However, it is comparatively easily possible to presume the cryptographic key used for that enciphered information by analyzing correlation with an attempt, each decode result, and the regularity between decode keys in decode of the information which prepared two or more decode keys with fixed regularity for the content also by this method, and was enciphered, using them every one, and its decode key. Therefore, there was a danger of decoding the enciphered information unjustly.

[0007] Moreover, although for example, the block cipher system, the public key system, etc. were variously proposed as an approach of solving these problems, all were complicated, and there was a problem that it was unsuitable for encryption processing of the information which has the need of reproducing on real time, such as a film and music, since decode processing takes time amount,

or expensive equipment was needed for it etc.

[0008] Then, this invention is comparatively easy, encryption and decode are cheaply possible for it, and, moreover, presumption of a decode key aims at offering the difficult information encryption approach, the information decryption approach, information encryption equipment, information decryption equipment, and an information record medium.

[0009]

[Means for Solving the Problem] As a means for attaining the above-mentioned object, the following information encryption approach, information decryption approaches, information encryption equipment, information decryption equipment, and information record media are offered.

[0010] 1. In Information Encryption Approach Which Enciphers Said Digital Information Data in case it Records on Information Record Medium with Sector Number Which Divides Digital Information Data into Two or More Sectors, and Shows Rank of Sector Carry out code conversion of the information key code of a proper to said digital information, and a work-piece key code is generated. The information encryption approach characterized by enciphering said digital information data which generated the encryption key code from this work-piece key code and said sector number, and were sector-ized using this encryption key code.

[0011] 2. In Information Decode Approach Which Decodes Said Digital Information Data of Record Medium with which Digital Information Data Which were Divided into Two or More Sectors and Enciphered are Recorded with Sector Number Which Shows Rank of Sector The information key code of a proper is decoded to said enciphered digital information which is supplied from other than said record medium. Carry out code conversion of this information key code, generate a work-piece key code, and a decryption key code is generated from this work-piece key code and said sector number currently recorded on said record medium. The information decode approach characterized by decoding the enciphered digital information which reproduces said record medium and is

acquired using this decryption key code.

[0012] 3. Divide Said Work-Piece Key Code into Two or More Partial Bit String of Numbers of Bits [ Code / Information Key ]. After carrying out exclusive logical addition of the one partial bit string of the arbitration chosen from this partial bit string to each of other partial bit string, respectively, combine it and the first bit string is generated. Carry out exclusive logical addition of said information key code and the second bit string of the same number of bits to said first bit string, and the third bit string is generated. After dividing into two or more partial bit strings of the numbers of bits [ bit string / said / third ] and carrying out low TETO only of the predetermined number of bits within each of this partial bit string on the right or the left, The information encryption approach of one above-mentioned publication characterized by generating the fourth bit string unitedly, dividing said fourth bit string into two or more partial bit strings, changing the array sequence of each partial bit string, and being generated, or the information decode approach of two above-mentioned publication.

[0013] 4. Said encryption key code or said decryption key code is the information encryption approach of one above-mentioned publication characterized by being the pseudo-random code train generated using the value just because it did the division of said work-piece key code with said sector number, or the information decode approach of two above-mentioned publication.

[0014] 5. In Information Encryption Equipment Which Enciphers Said Digital Information Data in case it Records on Information Record Medium with Sector Number Which Divides Digital Information Data into Two or More Sectors, and Shows Rank of Sector The code-conversion means which carries out code conversion of the information key code of a proper to said digital information, and carries out raw [ of the work-piece key code ], Information encryption equipment characterized by having an information encryption means to encipher said digital information data which generated the encryption key code from the work-piece key code outputted from this code-conversion means, and said sector number, and were sector-ized using this encryption key code.

[0015] 6. In Information Decode Equipment Which Decodes Said Digital Information Data of Record Medium with which Digital Information Data Which were Divided into Two or More Sectors and Enciphered are Recorded with Sector Number Which Shows Rank of Sector A key decode means to decode the information key code of a proper to said enciphered digital information which is supplied from other than said record medium, A code-conversion means to carry out code conversion of the information key code decoded with this key decode means, and to generate a work-piece key code, A decryption key code is generated from the work-piece key code generated with this code-conversion means, and said sector number currently recorded on said record medium. Information decode equipment characterized by having an information decryption means to decode the enciphered digital information which reproduces said record medium and is acquired using this decryption key code.

[0016] 7. Divide Said Code-Conversion Means into Two or More Partial Bit String of Numbers of Bits [ Code / Information Key ]. A bit string division / addition means to combine it and to generate the first bit string after carrying out exclusive logical addition of the one partial bit string of the arbitration chosen from this partial bit string to each of other partial bit string, respectively, An addition means to carry out exclusive logical addition of said information key code and the second bit string of the same number of bits to said first bit string, and to generate the third bit string, A bit rotation means to generate the fourth bit string unitedly after dividing into two or more partial bit strings of the numbers of bits [ bit string / said / third ] and carrying out low TETO only of the predetermined number of bits within each of this partial bit string on the right or the left, said fourth bit string -- two or more partial bit strings -- dividing -- the array sequence of each partial bit string -- changing -- work-piece key code **** -- the information encryption equipment of five above-mentioned publication characterized by things, or the information decode equipment of six above-mentioned publication.

[0017] 8. Said encryption key code or said decryption key code is the information encryption equipment of five above-mentioned publication characterized by being

the pseudo-random code train generated using the value just because it did the division of said work-piece key code with said sector number, or information decode equipment of six above-mentioned publication.

[0018] 9. It is the information record medium characterized by for the digital information data divided into two or more sectors being the information record medium currently recorded with the sector number which shows the rank of a sector, and enciphering said digital information data using the encryption key code generated from the work-piece key code which carried out code conversion of the information key code of a proper to said digital information, and said sector number.

[0019]

[Embodiment of the Invention] Before giving detailed explanation of the information encryption approach of this invention, the information decryption approach, information encryption equipment, information decryption equipment, and an information record medium, the outline of the information distribution system which is the field of the invention of this invention first is explained using drawing 1 .

[0020] In this drawing, the informational feeder has an information management means 1 to carry out generation management of the information key of a proper etc. to management of the information (contents) with which records on a record medium 3 and a sale etc. is presented, or information, and the customer management tool 5 which performs management of customer information, generation management of a distribution key or an authentication key, accounting management, etc.

[0021] And in supplying predetermined information to a predetermined customer First, while enciphering an information feeder using the authentication key which approves the information for which a customer asks to the information in encryption/record means 2, and approves informational acquisition to the information key and customer of a proper, recording on the predetermined information record medium 3 and supplying a customer It enciphers using a

distribution key as information for generating the decode key used in order to decode the enciphered information, and with the card issuance means 6, an information key, an authentication key, etc. are recorded on a card 7, and are distributed among a customer (or information corresponding to them etc.). A customer equips playback/decryption means 4 with the information record medium 3 and card 7 which were received, and acquires predetermined information. In addition, an authentication key is the information which the proper gave beforehand to the group to whom a customer or a customer belongs, and a distribution key is the information which the proper gave beforehand to information playback / decode equipment which a customer uses.

[0022] In such an information distribution system, this invention performs a new proposal about this encryption and decryption. That is, this invention divides digital information into two or more sectors, enciphers information for every sector using the cryptographic key generated based on the information key of a proper to the sector number and information which were given to each sector, and records the enciphered digital information data on a record medium.

[0023] Here, since a sector number is a number of a proper at each sector, each sector will use the cryptographic key of a proper for a sector, respectively, and will be enciphered. that is, information is enciphered using the cryptographic key frequently updated at intervals of about 0.003 seconds the example explained in full detail below. Thus, since a cryptographic key is updated at short spacing, it becomes very difficult to presume the cryptographic key used for it and its decode key from the enciphered information.

[0024] Moreover, in encryption and a decryption, an information key code is changed into another code, and the cryptographic key and the decode key are generated using the changed work-piece key code. Even if it is going to prepare two or more information keys which are mutually regular by this and is going to try presumption of a decode key, since regularity collapses, presumption of a decode key becomes difficult by this code conversion.

[0025] The case where DVD (Digital Versatile Disk) is used as a record medium

which records the enciphered information hereafter as one example of the information encryption approach of this invention, the information decryption approach, information encryption equipment, information decryption equipment, and an information record medium is explained. In addition, as an information record medium used by this invention, not only DVD but other magnetic tapes, a magnetic disk, etc. are effective.

[0026]

[Example] Drawing 2 is the block diagram showing the example of a configuration by the side of ****** supply with the encryption equipment of this invention. In this drawing, the information management means 1 is supplied to encryption/record means 2, in order to manage it, to encipher an information signal if needed and to record on a record medium, while holding as an inventory the information (it is also called contents information, such as image information, speech information, and data information, and following contents information) with which a sale etc. is presented. Moreover, in case an information signal is supplied to encryption/record means 2, the information key code which is the information on a proper is supplied to the contents information at encryption/record means 2 and the customer management tool 5.

[0027] In case the customer management tool 5 manages a distribution key, an authentication key, etc. and supplies contents information to a customer, it supplies an authentication key code to encryption/record means 2. Moreover, using a distribution key code, an information key code and an authentication key code are enciphered, and it outputs to the card record means 32, records on the card-like information record medium (it is hereafter described as a card) 7, and distributes among a customer (a user, information user). In addition, an authentication key is the information on the proper for identifying the group to whom a user or a user belongs (for example, a member number and a customer management number), and a distribution key is the information on the proper for identifying information playback / decode means 4 which a user uses (for example, identification numbers, such as a serial number of equipment).

[0028] The information signal supplied to encryption/record means 2 from the information management means 1 is first inputted into MPEG coding / sector-ized means 8. MPEG coding / sector-ized means 8 performs compression coding according the inputted information signal to an MPEG method, generates digital information data, and divides this digital information data into two or more sectors which consist of 2048 bytes further.

[0029] Then, in order to double with a DVD format, sector management information, a sector number, etc. are added to each sector, the data sector which consists of 2064 bytes is built, and encryption means 11a is supplied one by one.

[0030] The structure of the data sector built with this MPEG coding / sector-ized means 8 is shown in drawing 4 . 1 data sector shown in drawing 4 (b) consists of EDC (4 bytes) which is the error detection signs of IED (2 bytes) which is the error detection sign of ID data (4 bytes) and ID data, the Maine data (2048 bytes), and the Maine data. Furthermore, this ID data consists of sector information data (1 byte) and a sector number (3 bytes), as shown in drawing 4 (a). In addition, the sector-ized digital information data are contained by the above-mentioned Maine data area. Moreover, a sector number shows the rank of each data sector, and is usually the serial number from the first sector.

[0031] Moreover, the information key code supplied to encryption/record means 2 from the information management means 1 is inputted into code converter 9a. Moreover, the authentication key code supplied to encryption/record means 2 from the customer management tool 5 is also inputted into code converter 9a. And code converter 9a performs the predetermined operation and the code-conversion processing which are later mentioned between the information key codes and authentication key codes which were inputted, and supplies the work-piece key code obtained as a result to cryptographer stage 11a.

[0032] Here, although the information key code is used as one of the cryptographic key generation elements, the secrecy nature of a cryptographic key and a decode key is raised by changing into another code the information

key code supplied from the information management means 1. And the example of a configuration of code converter 9a is shown in drawing 6 , and the procedure of the operation and code-conversion processing is shown in drawing 7 . In the procedure of lower **, code conversion of the information key code is carried out, and it is outputted as a work-piece key code.

[0033] The information key code inputted is supplied to bit string division / adder 27. bit string division / adder 27 is arbitrary in the input code (information key code) supplied -- etc. -- it divides into two or more partial bit strings D0, D1, --, D9 which consist of bit length ( drawing 7 (a)). And exclusive logical addition of the one partial bit string (although it is D4 in the example, it does not restrict to this) is carried out according to an individual at each remaining partial bit strings, and the new partial bit strings (the first bit string) E0, E1, --, E9 are obtained. At this time, the exclusive OR of D4 comrades is E4, without taking. = It is referred to as D4. And these partial bit strings E0, E1, --, E9 are combined, a new bit string is obtained, and it outputs to an adder 30 ( drawing 7 (b)).

[0034] As opposed to the new bit string to which an adder 30 is supplied from bit string division / adder 27 the authentication key code ( drawing 7 (c) --) of the numbers of bits [ code / which is supplied from the customer management tool 5 / information key ] Exclusive logical addition of the second bit string is carried out, the obtained bit string is divided into two or more partial bit strings (the third bit string) F0, F1, --, F4 of bit length, such as arbitration, and it outputs to the bit rotation machine 28 ( drawing 7 (d)).

[0035] The bit rotation machine 28 is each partial bit string unit (inside of F0 and F1, --) divided in the partial bit strings F0, F1, --, F4 supplied, and only the predetermined number of bits carries out low TETO of it on the right ( drawing 7 (e)), and it obtains the partial bit strings G0, G1, --, G4 (the fourth bit string) ( drawing 7 (f)). These partial bit strings G0, G1, --, G4 are supplied to the bit string transposition machine 29, and change the array sequence of the partial bit strings G0, G1, --, G4 into arbitration. And it outputs to information encryption means 11a by using as a work-piece key code the bit string obtained as a result

( drawing 7 (g)).

[0036] Since it has the description said that a work-piece key code changes at random corresponding to it even if code converter 9a explained above changes an input key code into the work-piece key code of a meaning and an input key code changes regularly, it is very difficult to guess the decode key for decoding it from the information enciphered using such a work-piece key code.

[0037] In addition, although above-mentioned bit length, the above-mentioned number of partitions, etc. of each partial bit string are arbitrary, it is necessary to consider as the same bit length as code-conversion means 9b used with a playback/decode means 4 to mention later, and the partial bit string of the number of partitions.

[0038] Based on the work-piece key code supplied from code converter 9a, information encryption means 11a enciphers the sector data supplied from MPEG coding / sector-ized means 8, and supplies the enciphered sector data to ECC coding / modulation means 12.

[0039] Here, the example of a configuration of information encryption means 11a is shown in drawing 5 , and the actuation is explained, referring to drawing 4 . In this drawing, sector data are inputted into the signal divider 22 and the sector decoder 23 as an input bit string. Moreover, a work-piece key code is inputted into a divider 21.

[0040] The sector decoder 23 carries out detection decode of the ID data in sector data, and when an input bit string is during the Maine data area period, it supplies a division control signal ( drawing 4 (d)) to the signal divider 22. Moreover, a sector number is extracted and it outputs to a divider 21. Furthermore, an initialization control signal ( drawing 4 (c)) is supplied to M train coder 24 at the initiation event (before the Maine data area period comes) of each sector.

[0041] The signal divider 22 supplies the other data to the signal coupler 25 while supplying the Maine data in sector data to an adder 26 according to the division control signal supplied from the sector decoder 23.

[0042] On the other hand, the divider 21 is supplied to the M sequence coder 24 by making a value into initial value just because it did the division of the work-piece key code and obtained it as a result with the sector number supplied from the sector decoder 23. The M sequence coder 24 generates a pseudo-random code train (encryption key code) by making a value into initial value just because it is supplied from a divider 21, whenever an initialization control signal is supplied from the sector decoder 23, and it outputs it to an adder 26.

[0043] By carrying out exclusion logical addition of the pseudo-random code supplied from the M sequence coder 24 to the Maine data supplied from the signal divider 22, an adder 26 enciphers these and supplies the enciphered Maine data to the signal coupler 25. The signal coupler 25 outputs the sector data ( drawing 4 (e)) which combined ID data, IED data and copyright management information data which are supplied from the signal divider 22, and the enciphered Maine data which are supplied from an adder 26, and were enciphered.

[0044] Here, the sector number in ID data is the value of a proper like previous statement at each sector. Therefore, the M sequence coder 24 will generate a pseudo-random code train by making the value of a proper into initial value for every sector at the sector. Therefore, each sector is enciphered in a code train different, respectively.

[0045] Moreover, 1 sector is 2064-byte length like previous statement, and this is equivalent to a 0.003-second about room by real-time playback. That is, an encryption pattern will change one after another at intervals of about 0.003 seconds. Therefore, even if it reproduces the enciphered data which were recorded on the information record medium, it analyzes the data pattern and it tries decode of a cryptographic key / decode key, it is difficult to decode for such a short period of time.

[0046] Thus, information encryption means 11a outputs the sector data stream enciphered for every data sector to EC coding / modulator 12. And predetermined processing is performed to the enciphered sector data stream

which was outputted from information encryption machine 11a by well-known EC coding / modulator 12, and the well-known format means 13, and it is recorded on a master disc 14. Furthermore, based on this master disc 14, the well-known disk duplicate means 15 is used, the disk 16 for playback is reproduced, and a user is supplied. In addition, when you do not need many disks 16 for playback, you may use a master disc 14 as an object for user supply.

[0047] Furthermore, by key encryption means 31a, an information provider enciphers an above-mentioned information key code and an above-mentioned authentication key code using a distribution key code, respectively, supplies the card record means 32, and records on a card 7. And the card 7 which recorded the information key code and authentication key code which did in this way and were enciphered in distribution key code is distributed among a user. In addition, the technique, the card record means 32, and card 7 of encryption do not need to be a specific thing, and can use various things. [ a / key encryption means 31]

[0048] Drawing 3 is drawing showing the example of a configuration by the side of a user (information user side). A user equips playback/decode means 4 with the disk 16 for playback (information record medium) with which the enciphered contents information was recorded, and the card 7 with which information required in order to decode the enciphered information was recorded, and does the playback decode of the enciphered contents information.

[0049] A well-known information playback means 17 for playback/decode means 4 shown in this drawing to read data in the disk 16 for playback, and to output digital data, Well-known recovery / error correction means 18 which restores to information while carrying out an error correction using IED and EDC which are contained in a data sector, It consists of information decryption means 11b, the card decode means 19, the distribution key storing means 33, key decode means 31b, code converter 9b, and well-known well-known sector decomposition / MPEG decode means 20. In addition, with code converter 9a and information encryption means 11a in encryption/record means 2 as stated above, code converter 9b and information decryption means 11b are completely the same

configurations, and have the same actuation and the same function, respectively.

[0050] The playback means 17 supplies the playback information which was reproduced and was acquired from the disk 16 for playback to a recovery / error correction means 18. A recovery / error correction means 18 restores to playback information, carries out error correction processing, obtains the enciphered sector data, and supplies them to information decryption means 11b.

[0051] On the other hand, the card decode means 19 reads the enciphered information key code and the enciphered authentication key code which is recorded on the card 7, and supplies these to key decode means 31b.

[0052] Key decode means 31b decodes the information key code and authentication key code which are enciphered using the distribution key stored in the distribution key storing means 33, respectively, and outputs an information key code and an authentication key code to code converter 9b. In addition, the distribution keys stored in the distribution key storing means 33 are the identification numbers (for example, serial number etc.) of the equipment beforehand given to playback/decode means 4, and the same thing as the distribution key stored in the customer management tool 5 is used. In addition, the card decode means 19 and key decode means 31b can use various things and approaches.

[0053] The example of a configuration of code converter 9b is shown in drawing 6 . Since it is the configuration as code converter 9a used with encryption/record means 2 as stated above with this same, detailed explanation of the actuation is omitted. And the information key code similarly supplied from key decode means 31b is changed into a work-piece key code using the authentication key code supplied from key decode means 31b, and this is outputted to information decode means 11b.

[0054] The example of a configuration of information decryption means 11b is shown in drawing 5 . Although this is the same configuration as information encryption means 11a as stated above and the detailed explanation is omitted, the pseudo-random code train outputted from the M sequence sign generating

means 24 is used as a decode key code. Therefore, although the sector data which the sector data which should be enciphered as an input bit string were inputted in information encryption means 11a, and were enciphered as an output bit string are outputted, in information decryption means 11b, the sector data enciphered as an input bit string are inputted, and the sector data which decoded the sector data enciphered as an output bit string are outputted. here -- a work-piece key code -- the case of encryption, and the case of a decryption -- it is -- the same Cord -- certain ** Therefore, the enciphered sector data are decoded by the original sector data at accuracy.

[0055] And the decoded sector is outputted to sector separation / MPEG decode means 20, and MPEG decode is carried out and it is outputted to the original information signal.

[0056]

[Effect of the Invention] The information encryption approach of this invention, the information decode approach, information encryption equipment, and an information decode equipment information record medium can perform powerful encryption with an easy means.

[0057] And since the information record medium of this invention does not need to record the information about a cryptographic key / decode key, it does not need to secure the record section for it and is effective in the ability to use an informational record section efficiently.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing an example of an information distribution system.

[Drawing 2] It is the block diagram showing one example of the information

encryption equipment of this invention.

[Drawing 3] It is the block diagram showing one example of the information decode equipment of this invention.

[Drawing 4] It is drawing showing the example of the sector structure of the information recorded on the information record medium of this invention.

[Drawing 5] It is the block diagram showing one example of an information encryption means and an information decode means.

[Drawing 6] It is the block diagram showing one example of a code converter.

[Drawing 7] It is drawing for explaining an example of actuation by the code converter.

[Description of Notations]

1 Information Management Means

2 Encryption/Record Means

3 Information Record Medium

4 Playback/Decode Means

5 Customer Management Tool

6 Card Issuance Means

7 Card (Card-like Information Record Medium)

8 MPEG Coding / Sector-ized Means

9a, 9b Code converter (code-conversion means)

11a Information encryption means

11b Information decode means

12 ECC Coding / Modulation Means

13 Format Means

14 Master Disc

15 Disk Duplicate Means

16 Disk for Playback

17 Information Playback Means

18 Recovery / Error Correction Means

19 Card Decode Means

20 Sector Separation / MPEG Decode Means

21 Divider

22 Signal Division Means

23 Sector Decode Means

24 M Sequence Coder

25 Signal Coupling Means

26 Adder

27 Bit String Division / Adder

28 Bit Rotation Means

29 Bit String Transposition Means

30 Adder

31a Key encryption means

31b Key decode means

32 Card Record Means

33 Distribution Key Storing Means

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－195269

(43)公開日　平成11年(1999)７月21日

| (51)Int.Cl.[6] | 識別記号 | ＦＩ | |
|---|---|---|---|
| Ｇ１１Ｂ　20/10 | | Ｇ１１Ｂ　20/10 | Ｈ |
| Ｇ０９Ｃ　1/00 | ６１０ | Ｇ０９Ｃ　1/00 | ６１０Ｚ |
| | ６６０ | | ６６０Ｄ |
| Ｈ０４Ｌ　9/16 | | Ｈ０４Ｌ　9/00 | ６４３ |
| // Ｇ０６Ｆ　17/60 | | Ｇ０６Ｆ　15/21 | ３４０Ｚ |

審査請求　未請求　請求項の数９　ＦＤ　（全９頁）

(21)出願番号　特願平9－369395

(22)出願日　平成９年(1997)12月26日

(71)出願人　000004329
日本ビクター株式会社
神奈川県横浜市神奈川区守屋町３丁目12番地

(72)発明者　平田　渥美
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内

(72)発明者　町田　豊隆
千葉県柏市篠籠田1135－１　サルビア703

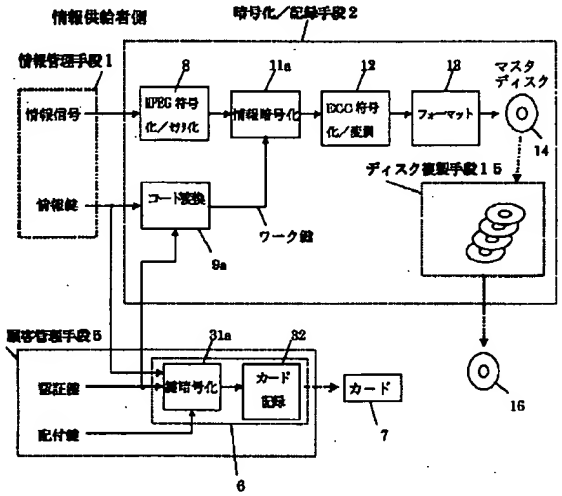
(72)発明者　廣田　昭
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内

(54)【発明の名称】　情報暗号化方法、情報復号方法、情報暗号化装置、情報復号装置及び情報記録媒体

(57)【要約】

【課題】　比較的簡単で安価に暗号化及び復号が可能で、しかも復号鍵の推定が困難な情報暗号化方法がなかった。

【解決手段】　情報管理手段１は、デジタル情報に固有の情報鍵コードと情報信号とを蓄積している。また、顧客管理手段５は、顧客固有の認証鍵と再生装置固有の配付鍵を蓄積している。そして、コード変換手段９ａにより情報鍵コードをコード変換してワーク鍵コードを生成する。さらに、情報暗号化手段１１ａでは、コード変換手段９ａより出力されるワーク鍵コードとセクタ番号とから暗号化鍵コードを生成し、この暗号化鍵コードを使用してセクタ化されたデジタル情報データを暗号化する。



【特許請求の範囲】
【請求項１】デジタル情報データを複数のセクタに分割してセクタの序列を示すセクタ番号と共に情報記録媒体に記録する際に前記デジタル情報データを暗号化する情報暗号化方法において、
前記デジタル情報に固有の情報鍵コードをコード変換してワーク鍵コードを生成し、
このワーク鍵コードと前記セクタ番号とから暗号化鍵コードを生成し、
この暗号化鍵コードを使用してセクタ化された前記デジタル情報データを暗号化することを特徴とする情報暗号化方法。
【請求項２】複数のセクタに分割されて暗号化されたデジタル情報データがセクタの序列を示すセクタ番号と共に記録されている記録媒体の前記デジタル情報データを復号する情報復号方法において、
前記記録媒体以外から供給される暗号化された前記デジタル情報に固有の情報鍵コードを復号し、
この情報鍵コードをコード変換してワーク鍵コードを生成し、
このワーク鍵コードと前記記録媒体に記録されている前記セクタ番号とから復号化鍵コードを生成し、
この復号化鍵コードを使用して前記記録媒体を再生して得られる暗号化されたデジタル情報を復号することを特徴とする情報復号方法。
【請求項３】前記ワーク鍵コードは、
情報鍵コードを等ビット数の複数部分ビット列に分割し、この部分ビット列から選択される任意の一つの部分ビット列を、それぞれ他の各部分ビット列に排他的論理加算してから結合して第一のビット列を生成し、
前記第一のビット列に前記情報鍵コードと同じビット数の第二のビット列を排他的論理加算して第三のビット列を生成し、
前記第三のビット列を等ビット数の複数の部分ビット列に分割し、この各部分ビット列内で所定のビット数だけ右又は左にローテートした後、結合して第四のビット列を生成し、
前記第四のビット列を複数の部分ビット列に分割し、各部分ビット列の配列順序を変更して生成されることを特徴とする請求項１記載の情報暗号化方法又は請求項２記載の情報復号方法。
【請求項４】前記暗号化鍵コード又は前記復号化鍵コードは、前記ワーク鍵コードを前記セクタ番号で除算した余り値を使用して発生した擬似ランダムコード列であることを特徴とする請求項１記載の情報暗号化方法又は請求項２記載の情報復号方法。
【請求項５】デジタル情報データを複数のセクタに分割してセクタの序列を示すセクタ番号と共に情報記録媒体に記録する際に前記デジタル情報データを暗号化する情報暗号化装置において、
前記デジタル情報に固有の情報鍵コードをコード変換してワーク鍵コードを生するコード変換手段と、
このコード変換手段より出力されるワーク鍵コードと前記セクタ番号とから暗号化鍵コードを生成し、この暗号化鍵コードを使用してセクタ化された前記デジタル情報データを暗号化する情報暗号化手段とを有することを特徴とする情報暗号化装置。
【請求項６】複数のセクタに分割されて暗号化されたデジタル情報データがセクタの序列を示すセクタ番号と共に記録されている記録媒体の前記デジタル情報データを復号する情報復号装置において、
前記記録媒体以外から供給される暗号化された前記デジタル情報に固有の情報鍵コードを復号する鍵復号手段と、
この鍵復号手段にて復号された情報鍵コードをコード変換してワーク鍵コードを生成するコード変換手段と、
このコード変換手段にて生成されたワーク鍵コードと前記記録媒体に記録されている前記セクタ番号とから復号化鍵コードを生成し、この復号化鍵コードを使用して前記記録媒体を再生して得られる暗号化されたデジタル情報を復号する情報復号化手段とを有することを特徴とする情報復号装置。
【請求項７】前記コード変換手段は、
情報鍵コードを等ビット数の複数部分ビット列に分割し、この部分ビット列から選択される任意の一つの部分ビット列を、それぞれ他の各部分ビット列に排他的論理加算してから結合して第一のビット列を生成するビット列分割／加算手段と、
前記第一のビット列に前記情報鍵コードと同じビット数の第二のビット列を排他的論理加算して第三のビット列を生成する加算手段と、
前記第三のビット列を等ビット数の複数の部分ビット列に分割し、この各部分ビット列内で所定のビット数だけ右又は左にローテートした後、結合して第四のビット列を生成するビットローテーション手段と、
前記第四のビット列を複数の部分ビット列に分割し、各部分ビット列の配列順序を変更してワーク鍵コード得ることを特徴とする請求項５記載の情報暗号化装置又は請求項６記載の情報復号装置。
【請求項８】前記暗号化鍵コード又は前記復号化鍵コードは、前記ワーク鍵コードを前記セクタ番号で除算した余り値を使用して発生した擬似ランダムコード列であることを特徴とする請求項５記載の情報暗号化装置又は請求項６記載の情報復号装置。
【請求項９】複数のセクタに分割されたデジタル情報データがセクタの序列を示すセクタ番号と共に記録されている情報記録媒体であって、
前記デジタル情報データは、前記デジタル情報に固有の情報鍵コードをコード変換したワーク鍵コードと前記セクタ番号とから生成される暗号化鍵コードを使用して暗

号化されていることを特徴とする情報記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報の暗号化／復号方法に係り、特に、映像信号、音声信号、データ信号等の情報をセクタ化して、ディスク等の情報記録媒体に記録／再生を行う場合に用いて好適な情報暗号化方法、情報復号方法、情報暗号化装置、情報復号装置及び情報記録媒体に関するものである。

【０００２】

【従来の技術】従来より、所定の記録媒体に情報を暗号化して記録する場合、所定の暗号化鍵を用いて情報を暗号化して所定の記録媒体に記録すると同時に、暗号化された情報を復号するための復号鍵（あるいは復号鍵に対応する情報）を、同一記録媒体に記録している。この場合、復号鍵（あるいは復号鍵に対応する情報）は、記録媒体の所定の連続した領域に連続して記録、あるいは、連続しない複数の領域に分散して記録している。

【０００３】復号は、記録媒体から再生して得た復号鍵、あるいは復号鍵に対応する情報を基に生成した復号鍵を用いて、同じ記録媒体から再生される暗号化された情報を復号していた。

【０００４】また、暗号化は、少なくとも一つの情報については一つの暗号鍵を用いて暗号化している。例えば、60分間長の映画の情報を暗号化する場合、60分間全編に亙って同一の暗号鍵を用いて暗号化していた。

【０００５】

【発明が解決しようとする課題】従来は、暗号化された情報と、その暗号化された情報を復号するために用いる復号鍵（あるいは復号鍵に対応する情報）とが、同一の記録媒体に記録されており、また一つの情報全体に亙って同一暗号鍵を用いて暗号化しているため、復号鍵を推定され易いという課題があった。また、情報記録媒体内に、復号鍵（あるいは復号鍵に対応する情報）を記録しているので、情報記録媒体内にそのための領域を確保する必要があり、その分、本来の情報を記録する領域が減少していた。

【０００６】なお、比較的簡単で且つ効果的な暗号化／復号化方法として、共通鍵方式によるPN加算方式がある。この方式は、擬似ランダム加算方式とも呼ばれ、M系列符号発生器を利用して情報を暗号化するものである。しかし、この方式でも、内容に一定の規則性がある複数個の復号鍵を準備し、それらを一つづつ用いて、暗号化された情報の復号を試み、個々の復号結果と、復号鍵間の規則性との相関を解析することによって、その暗号化された情報に用いられた暗号鍵及びその復号鍵を推定することが比較的容易に可能である。したがって、暗号化された情報を不正に解読される危険性があった。

【０００７】また、これらの問題を解決する方法として、例えば、ブロック暗号化方式、公開鍵方式等種々提案されているが、いずれも複雑で復号処理に時間が掛かるので、映画や音楽などのリアルタイムで再生する必要のある情報の暗号化処理には不向きであったり、高価な装置が必要になったりする等の問題があった。

【０００８】そこで本発明は、比較的簡単で安価に暗号化及び復号が可能で、しかも復号鍵の推定が困難な情報暗号化方法、情報復号化方法、情報暗号化装置、情報復号化装置及び情報記録媒体を提供することを目的とする。

【０００９】

【課題を解決するための手段】上記目的を達成するための手段として、以下の情報暗号化方法、情報復号化方法、情報暗号化装置、情報復号化装置及び情報記録媒体を提供する。

【００１０】１．デジタル情報データを複数のセクタに分割してセクタの序列を示すセクタ番号と共に情報記録媒体に記録する際に前記デジタル情報データを暗号化する情報暗号化方法において、前記デジタル情報に固有の情報鍵コードをコード変換してワーク鍵コードを生成し、このワーク鍵コードと前記セクタ番号とから暗号化鍵コードを生成し、この暗号化鍵コードを使用してセクタ化された前記デジタル情報データを暗号化することを特徴とする情報暗号化方法。

【００１１】２．複数のセクタに分割されて暗号化されたデジタル情報データがセクタの序列を示すセクタ番号と共に記録されている記録媒体の前記デジタル情報データを復号する情報復号方法において、前記記録媒体以外から供給される暗号化された前記デジタル情報に固有の情報鍵コードを復号し、この情報鍵コードをコード変換してワーク鍵コードを生成し、このワーク鍵コードと前記記録媒体に記録されている前記セクタ番号とから復号化鍵コードを生成し、この復号化鍵コードを使用して前記記録媒体を再生して得られる暗号化されたデジタル情報を復号することを特徴とする情報復号方法。

【００１２】３．前記ワーク鍵コードは、情報鍵コードを等ビット数の複数部分ビット列に分割し、この部分ビット列から選択される任意の一つの部分ビット列を、それぞれ他の各部分ビット列に排他的論理加算してから結合して第一のビット列を生成し、前記第一のビット列に前記情報鍵コードと同じビット数の第二のビット列を排他的論理加算して第三のビット列を生成し、前記第三のビット列を等ビット数の複数の部分ビット列に分割し、この各部分ビット列内で所定のビット数だけ右又は左にローテートした後、結合して第四のビット列を生成し、前記第四のビット列を複数の部分ビット列に分割し、各部分ビット列の配列順序を変更して生成されることを特徴とする上記１記載の情報暗号化方法又は上記２記載の情報復号方法。

【００１３】４．前記暗号化鍵コード又は前記復号化鍵コードは、前記ワーク鍵コードを前記セクタ番号で除算

した余り値を使用して発生した擬似ランダムコード列であることを特徴とする上記１記載の情報暗号化方法又は上記２記載の情報復号方法。

【００１４】５．デジタル情報データを複数のセクタに分割してセクタの序列を示すセクタ番号と共に情報記録媒体に記録する際に前記デジタル情報データを暗号化する情報暗号化装置において、前記デジタル情報に固有の情報鍵コードをコード変換してワーク鍵コードを生するコード変換手段と、このコード変換手段より出力されるワーク鍵コードと前記セクタ番号とから暗号化鍵コードを生成し、この暗号化鍵コードを使用してセクタ化された前記デジタル情報データを暗号化する情報暗号化手段とを有することを特徴とする情報暗号化装置。

【００１５】６．複数のセクタに分割されて暗号化されたデジタル情報データがセクタの序列を示すセクタ番号と共に記録されている記録媒体の前記デジタル情報データを復号する情報復号装置において、前記記録媒体以外から供給される暗号化された前記デジタル情報に固有の情報鍵コードを復号する鍵復号手段と、この鍵復号手段にて復号された情報鍵コードをコード変換してワーク鍵コードを生成するコード変換手段と、このコード変換手段にて生成されたワーク鍵コードと前記記録媒体に記録されている前記セクタ番号とから復号化鍵コードを生成し、この復号化鍵コードを使用して前記記録媒体を再生して得られる暗号化されたデジタル情報を復号する情報復号化手段とを有することを特徴とする情報復号装置。

【００１６】７．前記コード変換手段は、情報鍵コードを等ビット数の複数部分ビット列に分割し、この部分ビット列から選択される任意の一つの部分ビット列を、それぞれ他の各部分ビット列に排他的論理加算してから結合して第一のビット列を生成するビット列分割／加算手段と、前記第一のビット列に前記情報鍵コードと同じビット数の第二のビット列を排他的論理加算して第三のビット列を生成する加算手段と、前記第三のビット列を等ビット数の複数の部分ビット列に分割し、この各部分ビット列内で所定のビット数だけ右又は左にローテートした後、結合して第四のビット列を生成するビットローテーション手段と、前記第四のビット列を複数の部分ビット列に分割し、各部分ビット列の配列順序を変更してワーク鍵コード得ることを特徴とする上記５記載の情報暗号化装置又は上記６記載の情報復号装置。

【００１７】８．前記暗号化鍵コード又は前記復号化鍵コードは、前記ワーク鍵コードを前記セクタ番号で除算した余り値を使用して発生した擬似ランダムコード列であることを特徴とする上記５記載の情報暗号化装置又は上記６記載の情報復号装置。

【００１８】９．複数のセクタに分割されたデジタル情報データがセクタの序列を示すセクタ番号と共に記録されている情報記録媒体であって、前記デジタル情報データは、前記デジタル情報に固有の情報鍵コードをコード変換したワーク鍵コードと前記セクタ番号とから生成される暗号化鍵コードを使用して暗号化されていることを特徴とする情報記録媒体。

【００１９】

【発明の実施の形態】本発明の情報暗号化方法、情報復号化方法、情報暗号化装置、情報復号化装置及び情報記録媒体の詳細な説明をするのに先だって、先ず本発明の利用分野である情報供給システムの概要について図１を用いて説明する。

【００２０】同図において、情報の供給者は、記録媒体３に記録して販売等に供する情報（コンテンツ）の管理や情報に固有の情報鍵の生成管理等を行う情報管理手段１と、顧客情報の管理、配付鍵や認証鍵の生成管理、課金管理等を行う顧客管理手段５とを有している。

【００２１】そして、所定の情報を所定の顧客に供給するに当たっては、まず、情報供給者は、暗号化／記録手段２において、顧客が所望する情報を、その情報に固有の情報鍵及び顧客に情報の取得を認可する認証鍵を用いて暗号化し、所定の情報記録媒体３に記録して顧客に供給する一方で、暗号化された情報を復号するために用いる復号鍵を生成するための情報として、情報鍵、認証鍵等（あるいは、それらに対応した情報等）を配付鍵を用いて暗号化し、カード発行手段６によってカード７に記録して、顧客に配付する。　顧客は受け取った情報記録媒体３及びカード７を再生／復号化手段４に装着して、所定の情報を取得する。なお、認証鍵は、顧客あるいは顧客が属するグループ等に固有の予め付与した情報であり、また、配付鍵は顧客が使用する情報再生／復号装置に固有の予め付与した情報である。

【００２２】このような情報供給システムにおいて本発明は、この暗号化および復号化に関して新たな提案を行うものである。すなわち、本発明は、デジタル情報を複数のセクタに分割し、各セクタに付与したセクタ番号及び情報に固有の情報鍵を基に生成した暗号鍵を用いて、各セクタ毎に情報を暗号化し、その暗号化したデジタル情報データを記録媒体に記録するものである。

【００２３】ここで、セクタ番号は各セクタに固有の番号であるため、各セクタはそれぞれセクタに固有の暗号鍵を用いて暗号化されることになる。すなわち、情報は、頻繁に（下記に詳述する実施例では約0.003秒間隔で）更新される暗号鍵を用いて暗号化される。この様に短い間隔で暗号鍵が更新されるため、暗号化された情報から、それに用いられた暗号鍵及びその復号鍵を推定することは極めて困難となる。

【００２４】また、暗号化及び復号化に当たって、情報鍵コードを別のコードに変換し、その変換されたワーク鍵コードを用いて暗号鍵及び復号鍵を生成している。これにより、互いに規則性のある複数個の情報鍵を準備して復号鍵の推定を試みようとしても、このコード変換によって、規則性が崩れるため復号鍵の推定が困難とな

る。

【００２５】以下、本発明の情報暗号化方法、情報復号化方法、情報暗号化装置、情報復号化装置及び情報記録媒体の一実施例として、暗号化された情報を記録する記録媒体としてＤＶＤ(Digital Versatile Disk)を用いた場合について説明する。なお、本発明で使用する情報記録媒体としては、ＤＶＤに限らず、他の磁気テープ、磁気ディスク等も有効である。

【００２６】

【実施例】図２は、本発明の暗号化装置でる情報供給側の構成例を示すブロック図である。同図において、情報管理手段１は、販売等に供する情報（映像情報、音声情報、データ情報等のコンテンツ情報、以下コンテンツ情報ともいう）を在庫として保有するとともにそれを管理し、必要に応じて情報信号を暗号化して記録媒体に記録するために、暗号化／記録手段２に供給するものである。また、情報信号を暗号化／記録手段２に供給する際には、そのコンテンツ情報に固有の情報である情報鍵コードを、暗号化／記録手段２及び顧客管理手段５に供給する。

【００２７】顧客管理手段５は、配付鍵、認証鍵等の管理を行い、コンテンツ情報を顧客に供給する際に、認証鍵コードを暗号化／記録手段２に供給する。　また、配付鍵コードを用いて、情報鍵コード及び認証鍵コードを暗号化し、カード記録手段３２に出力してカード状情報記録媒体（以下、カードと記す）７に記録して、顧客（ユーザ、情報利用者）に配付する。なお、認証鍵は、ユーザあるいはユーザが属するグループ等を識別するための固有の情報（例えば会員番号や顧客管理番号）であり、また、配付鍵はユーザが使用する情報再生／復号手段４を識別するための固有の情報（例えば装置の製造番号等の識別番号）である。

【００２８】情報管理手段１から暗号化／記録手段２に供給された情報信号は、まず、ＭＰＥＧ符号化／セクタ化手段８に入力される。ＭＰＥＧ符号化／セクタ化手段８は、入力された情報信号をＭＰＥＧ方式による圧縮符号化を行ってデジタル情報データを生成し、更に、このデジタル情報データを2048バイトから成る複数のセクタに分割する。

【００２９】その後、ＤＶＤフォーマットに合わせるために、各セクタにセクタ管理情報、セクタ番号等を付加して、2064バイトで構成されるデータセクタを構築し、順次、暗号化手段１１ａに供給する。

【００３０】このＭＰＥＧ符号化／セクタ化手段８で構築されるデータセクタの構造を図４に示す。図４（b）に示す１データセクタは、IDデータ(4バイト)、IDデータのエラー検出符号であるIED(2バイト)、メインデータ(2048バイト)及びメインデータのエラー検出符号であるEDC(4バイト)で構成されている。更に、このIDデータは図４（a）に示すように、セクタ情報データ(1バイト)とセクタ番号(3バイト)とで構成される。なお、セクタ化されたデジタル情報データは、上記のメインデータ領域に収納される。また、セクタ番号は、各データセクタの序列を示し、通常は最初のセクタからの通し番号である。

【００３１】また、情報管理手段１から暗号化／記録手段２に供給された情報鍵コードは、コード変換器９ａに入力される。また、顧客管理手段５から暗号化／記録手段２に供給された認証鍵コードも、コード変換器９ａに入力される。そして、コード変換器９ａは、入力された情報鍵コードと認証鍵コードとの間で後述する所定の演算及びコード変換処理を行ない、その結果得たワーク鍵コードを暗号手段１１ａに供給する。

【００３２】ここでは、情報鍵コードを暗号鍵生成要素の一つとして使用しているが、情報管理手段１から供給された情報鍵コードを、別のコードに変換することによって、暗号鍵および復号鍵の秘匿性を高めている。そして、図６にコード変換器9aの構成例を示し、図７にその演算及びコード変換処理の手順を示す。情報鍵コードは、下述の手順でコード変換されてワーク鍵コードとして出力される。

【００３３】入力される情報鍵コードは、ビット列分割／加算器２７に供給される。ビット列分割／加算器２７は、供給される入力コード（情報鍵コード）を任意の等ビット長からなる複数の部分ビット列D0, D1, …, D9に分割する（図７(a)）。そして、一つの部分ビット列（実施例ではD4であるが、これに限らない）を、残りの各部分ビット列に、個別に排他的論理加算して新たな部分ビット列（第一のビット列）E0, E1, …, E9を得る。この時、Ｄ４同士の排他的論理和は採らずにE4 = D4とする。そして、これらの部分ビット列E0, E1, …, E9を結合して新たなビット列を得て、加算器３０に出力する（図７(b)）。

【００３４】加算器３０は、ビット列分割／加算器２７から供給される新たなビット列に対して、顧客管理手段５から供給される情報鍵コードと等ビット数の認証鍵コード（図７(c)，第二のビット列）を排他的論理加算し、得られたビット列を任意の等ビット長の複数の部分ビット列（第三のビット列）F0, F1, …, F4に分割してビットローテーション器２８に出力する（図７(d)）。

【００３５】ビットローテーション器２８は、供給される部分ビット列F0, F1, …, F4を分割された各部分ビット列単位（F0内、F1内、…）で、所定のビット数だけ右にローテートし（図７(e)）、部分ビット列G0, G1, …, G4（第四のビット列）を得る（図７(f)）。この部分ビット列G0, G1, …, G4は、ビット列転置器２９に供給され、部分ビット列G0, G1, …, G4の配列順序を任意に変更する。そして、その結果得たビット列をワーク鍵コードとして情報暗号化手段１１ａに出力する（図７(g)）。

【００３６】以上説明したコード変換器９ａは、入力情

報鍵コードを一意のワーク鍵コードに変換し、入力情報鍵コードが規則的に変化しても、それに対応してワーク鍵コードはランダムに変化すると言う特徴を有して居るので、この様なワーク鍵コードを用いて暗号化された情報から、それを復号するための復号鍵を推測することは極めて困難である。

【００３７】なお、上記した各部分ビット列のビット長や分割数などは任意であるが、後述する再生／復号手段４で使用するコード変換手段９ｂと同じビット長及び分割数の部分ビット列とする必要がある。

【００３８】情報暗号化手段１１ａは、コード変換器９ａから供給されたワーク鍵コードに基づいて、ＭＰＥＧ符号化／セクタ化手段８から供給されたセクタデータを暗号化し、暗号化されたセクタデータをＥＣＣ符号化／変調手段１２に供給する。

【００３９】ここで、情報暗号化手段１１ａの構成例を図５に示し、図４を参照しながらその動作について説明する。同図において、セクタデータは、入力ビット列として信号分割器２２及びセクタ解読器２３に入力される。また、ワーク鍵コードは除算器２１に入力される。

【００４０】セクタ解読器２３は、セクタデータ内のIDデータを検出解読して、入力ビット列がメインデータ領域期間中である場合には、分割制御信号（図４(d)）を信号分割器22に供給する。また、セクタ番号を抽出して、除算器２１に出力する。さらに、各セクタの開始時点（メインデータ領域期間となる前）に、初期化制御信号（図４(c)）をM列符号発生器２４に供給する。

【００４１】信号分割器２２は、セクタ解読器23から供給される分割制御信号に応じて、セクタデータ内のメインデータを加算器２６に供給すると共に、それ以外のデータを信号結合器２５に供給する。

【００４２】一方、除算器２１は、セクタ解読器２３から供給されるセクタ番号でワーク鍵コードを除算し、その結果得た余り値を初期値としてM系列符号発生器２４に供給する。M系列符号発生器２４は、セクタ解読器２３から初期化制御信号が供給される度に、除算器２１から供給される余り値を初期値として、疑似ランダムコード列（暗号化鍵コード）を発生し、加算器２６に出力する。

【００４３】加算器２６は、信号分割器２２から供給されるメインデータに、M系列符号発生器２４から供給された疑似ランダムコードを排他論理加算することによってこれらを暗号化し、暗号化されたメインデータを信号結合器２５に供給する。信号結合器２５は、信号分割器２２から供給されるIDデータ、IEDデータ及び著作権管理情報データと、加算器２６から供給される暗号化されたメインデータとを結合して、暗号化されたセクタデータ（図４(e)）を出力する。

【００４４】ここで、IDデータ内のセクタ番号は、既述のごとく各セクタに固有の値である。したがって、M系列符号発生器２４は、各セクタ毎に、そのセクタに固有の値を初期値として疑似ランダムコード列を発生することになる。したがって、各セクタは、それぞれ異なるコード列で暗号化される。

【００４５】また、１セクタは、既述のごとく2064バイト長であり、これは実時間再生で0.003秒間程度に相当する。すなわち、暗号化パターンが約0.003秒間隔で次々と変わることになる。したがって、情報記録媒体に記録された暗号化されたデータを再生して、そのデータパターンを解析して暗号鍵／復号鍵の解読を試みても、この様な短期間に解読することは困難である。

【００４６】このようにして、情報暗号化手段１１ａは、各データセクタごとに暗号化されたセクタデータ列をＥＣ符号化／変調器１２に出力する。そして、情報暗号化器１１ａから出力された暗号化されたセクタデータ列は、公知のＥＣ符号化／変調器１２及び公知のフォーマット手段１３により所定の処理を施されて、マスタディスク１４に記録される。さらに、このマスタディスク１４を基に、公知ディスク複製手段１５を用いて、再生用ディスク１６を複製してユーザに供給する。なお、多くの再生用ディスク１６を必要としない場合には、マスタディスク１４をユーザ供給用として使用しても良い。

【００４７】さらに、情報提供者は、鍵暗号化手段３１ａにより、前述の情報鍵コード及び認証鍵コードを配付鍵コードを用いてそれぞれ暗号化し、カード記録手段３２に供給してカード７に記録する。そして、このようにして配付鍵コードで暗号化された情報鍵コード及び認証鍵コードを記録したカード７をユーザに配付する。なお、鍵暗号化手段３１ａでの暗号化の手法やカード記録手段３２及びカード７は特定のものである必要はなく、種々のものを使用することができる。

【００４８】図３は、ユーザ側（情報利用者側）の構成例を示す図である。ユーザは、暗号化されたコンテンツ情報が記録された再生用ディスク（情報記録媒体）１６と、暗号化された情報を復号するために必要な情報が記録されたカード７とを再生／復号手段４に装着して、暗号化されたコンテンツ情報を再生復号する。

【００４９】同図に示す再生／復号手段４は、再生用ディスク１６からデータを読み取ってデジタルデータを出力する公知の情報再生手段１７と、データセクタに含まれるＩＥＤやＥＤＣを使用してエラー訂正をすると共に情報の復調を行う公知の復調／エラー訂正手段１８と、情報復号化手段１１ｂと、カード解読手段１９と、配付鍵格納手段３３と、鍵復号手段３１ｂと、コード変換器９ｂ及び公知のセクタ分解／ＭＰＥＧ復号手段２０で構成されている。なお、コード変換器９ｂ及び情報復号化手段１１ｂは、それぞれ、既述の暗号化／記録手段２における、コード変換器９ａ及び情報暗号化手段１１ａと全く同一構成であり、同一動作及び同一機能を有している。

【００５０】再生手段１７は、再生用ディスク１６から再生して得た再生情報を、復調／エラー訂正手段１８に供給する。復調／エラー訂正手段１８は、再生情報を復調してエラー訂正処理し、暗号化されたセクタデータを得て情報復号化手段１１ｂに供給する。

【００５１】一方、カード解読手段１９は、カード7に記録されている暗号化された情報鍵コード及び暗号化された認証鍵コードを読み出し、これらを鍵復号手段３１ｂに供給する。

【００５２】鍵復号手段３１ｂは、配付鍵格納手段３３に格納されている配付鍵を用いて、暗号化されている情報鍵コードと認証鍵コードをそれぞれ復号して、情報鍵コードと認証鍵コードとをコード変換器９ｂに出力する。なお、配付鍵格納手段３３に格納されている配付鍵は、再生／復号手段４に予め付与された装置の識別番号（例えば製造番号等）であり、顧客管理手段５に格納されている配付鍵と同一のものが使用される。なお、カード解読手段１９及び鍵復号手段３１ｂは種々のもの及び方法を使用することができる。

【００５３】コード変換器９ｂの構成例を図６に示す。これは、既述の暗号化／記録手段２で用いたコード変換器９ａと同一構成であるので、その動作の詳細な説明は省略する。そして、鍵復号手段３１ｂから供給される認証鍵コードを用いて、同じく鍵復号手段３１ｂから供給される情報鍵コードをワーク鍵コードに変換し、これを情報復号手段１１ｂに出力する。

【００５４】図５に情報復号化手段１１ｂの構成例を示す。これは既述の情報暗号化手段１１ａと同一構成であり、その詳細な説明は省略するが、M系列符号発生手段２４から出力される擬似ランダムコード列は復号鍵コードとして使用される。したがって、情報暗号化手段１１ａの場合は、入力ビット列として暗号化するべきセクタデータが入力され、出力ビット列として暗号化されたセクタデータが出力されるが、情報復号化手段１１ｂでは、入力ビット列として暗号化されたセクタデータが入力され、出力ビット列として暗号化されたセクタデータを復号したセクタデータが出力される。ここで、ワーク鍵コードは、暗号化の場合と復号化の場合とで、同一コードある。したがって、暗号化されたセクタデータは、正確に元のセクタデータに復号される。

【００５５】そして、復号されたセクタは、セクタ分離／ＭＰＥＧ復号手段２０に出力され、元の情報信号にＭＰＥＧ復号されて出力される。

【００５６】

【発明の効果】本発明の情報暗号化方法、情報復号方法、情報暗号化装置及び情報復号装置情報記録媒体は、簡単な手段で強力な暗号化を行うことができる。

【００５７】そして、本発明の情報記録媒体は、暗号鍵／復号鍵に関する情報を記録する必要がないので、そのための記録領域を確保する必要なく、情報の記録領域を効率よく使用することができるという効果がある。

【図面の簡単な説明】

【図１】情報供給システムの一例を示す構成図である。

【図２】本発明の情報暗号化装置の一実施例を示す構成図である。

【図３】本発明の情報復号装置の一実施例を示す構成図である。

【図４】本発明の情報記録媒体に記録する情報のセクタ構造の例を示す図である。

【図５】情報暗号化手段及び情報復号手段の一実施例を示す構成図である。

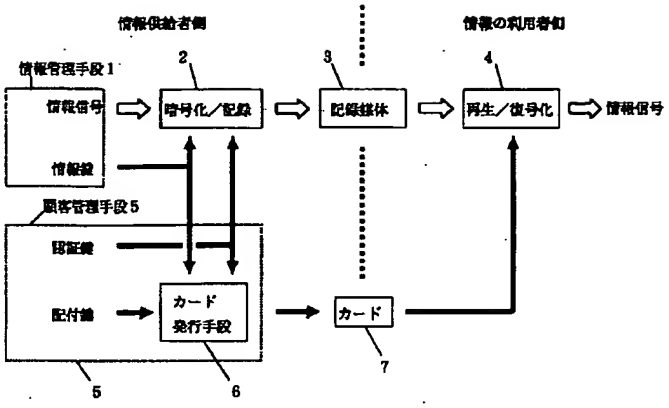
【図６】コード変換器の一実施例を示す構成図である。

【図７】コード変換器での動作の一例を説明するための図である。

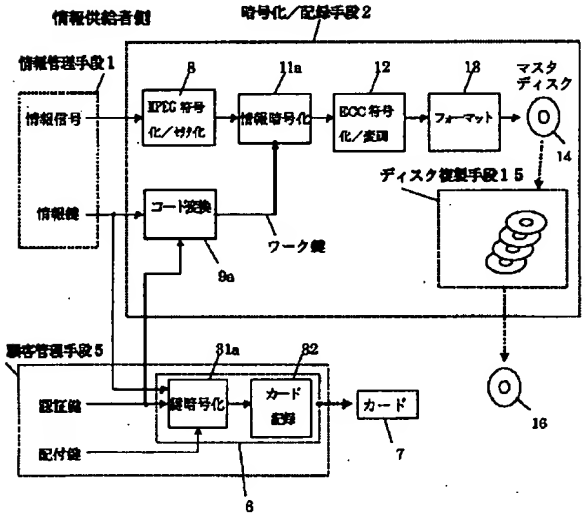
【符号の説明】

１　情報管理手段
２　暗号化／記録手段
３　情報記録媒体
４　再生／復号手段
５　顧客管理手段
６　カード発行手段
７　カード（カード状情報記録媒体）
８　ＭＰＥＧ符号化／セクタ化手段
９ａ，９ｂ　コード変換器（コード変換手段）
１１ａ　情報暗号化手段
１１ｂ　情報復号手段
１２　ＥＣＣ符号化／変調手段
１３　フォーマット手段
１４　マスタディスク
１５　ディスク複製手段
１６　再生用ディスク
１７　情報再生手段
１８　復調／エラー訂正手段
１９　カード解読手段
２０　セクタ分離／ＭＰＥＧ復号手段
２１　除算器
２２　信号分割手段
２３　セクタ解読手段
２４　M系列符号発生器
２５　信号結合手段
２６　加算器
２７　ビット列分割／加算器
２８　ビットローテーション手段
２９　ビット列転置手段
３０　加算器
３１ａ　鍵暗号化手段
３１ｂ　鍵復号手段
３２　カード記録手段
３３　配付鍵格納手段

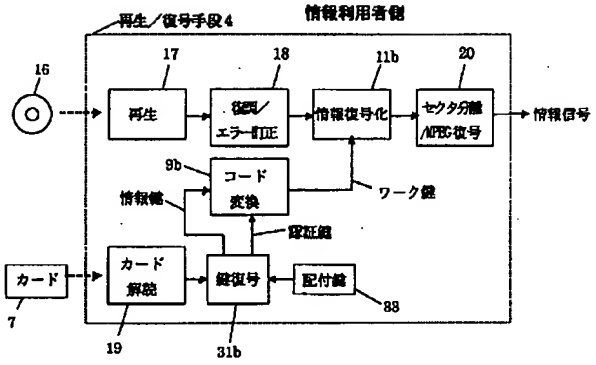
【図１】


情報供給者側
情報の利用者側
情報管理手段１
2
3
4
情報信号
暗号化／記録
記録媒体
再生／復号化
情報信号
情報鍵
顧客管理手段５
認証鍵
配付鍵
カード
発行手段
カード
5
6
7

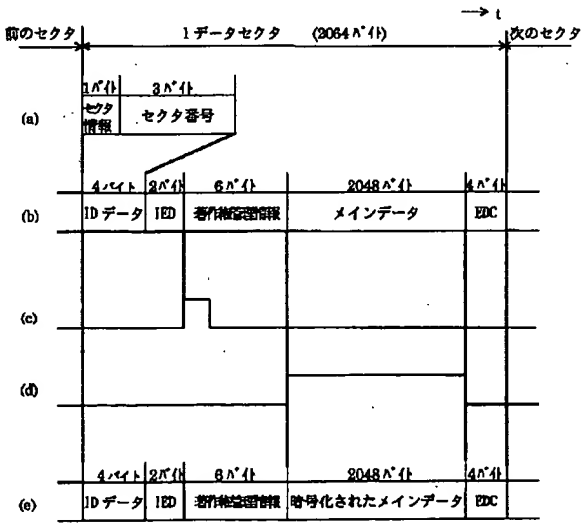
【図２】


情報供給者側
暗号化／記録手段２
情報管理手段１
8
11a
12
13
マスタ
ディスク
MPEG符号
化／ｻﾌｧ化
情報暗号化
ECC符号
化／変調
フォーマット
情報信号
14
ディスク複製手段１５
情報鍵
コード変換
ワーク鍵
9a
顧客管理手段５
31a
82
認証鍵
鍵暗号化
カード
記録
カード
配付鍵
7
6
16

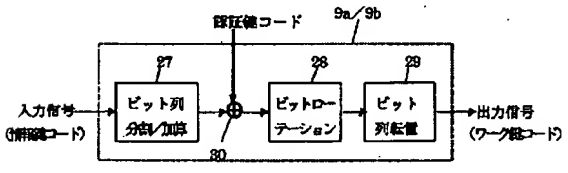
【図３】


再生／復号手段４
情報利用者側
16
17
18
11b
20
再生
復調／
エラー訂正
情報復号化
セクタ分離
/MPEG復号
情報信号
9b
コード
変換
情報鍵
ワーク鍵
認証鍵
カード
カード
解説
鍵復号
配付鍵
83
7
19
31b

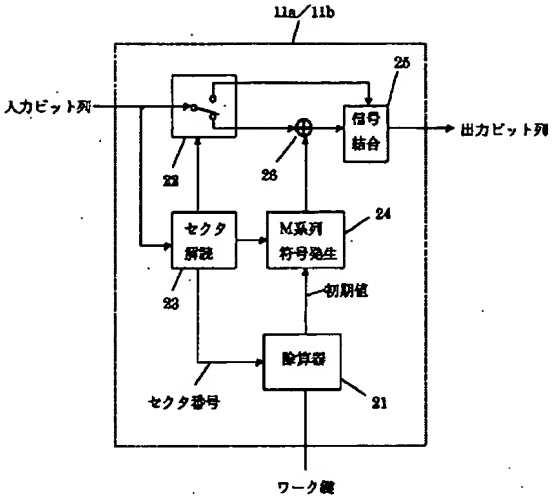
【図４】


t
前のセクタ
1データセクタ　(2064バイト)
次のセクタ
(a)
1バイト
セクタ情報
3バイト
セクタ番号
(b)
4バイト
2バイト
6バイト
2048バイト
4バイト
IDデータ
IED
著作権管理情報
メインデータ
EDC
(c)
(d)
(e)
暗号化されたメインデータ

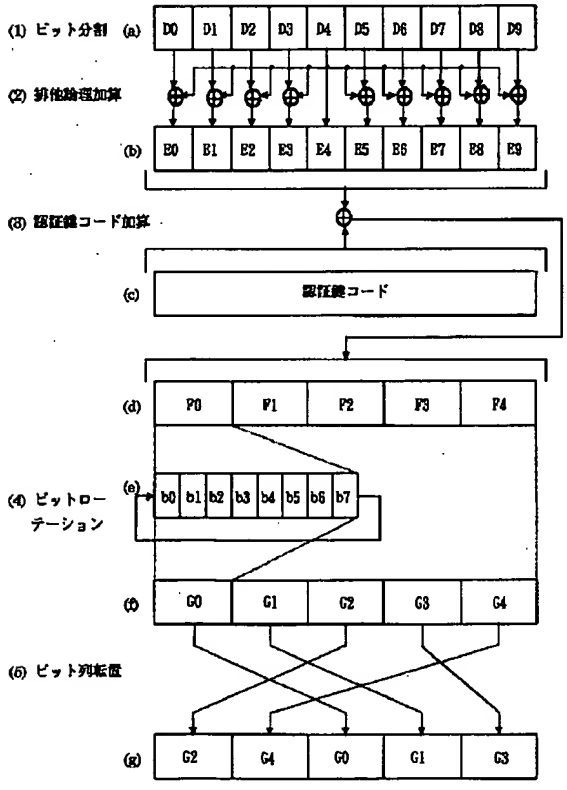
【図６】


認証鍵コード
9a／9b
27
28
29
入力信号
(情報鍵コード)
ビット列
分割/加算
ビットロー
テーション
ビット
列転置
出力信号
(ワーク鍵コード)
30

【図５】


11a/11b
25
入力ビット列
信号結合
出力ビット列
22
26
セクタ解読
M系列符号発生
24
23
初期値
除算器
セクタ番号
21
ワーク領

【図７】


(1) ビット分割 (a)
D0 D1 D2 D3 D4 D5 D6 D7 D8 D9
(2) 排他論理加算
(b)
E0 E1 E2 E3 E4 E5 E6 E7 E8 E9
(3) 認証鍵コード加算
(c)
認証鍵コード
(d)
F0 F1 F2 F3 F4
(4) ビットローテーション
(e)
b0 b1 b2 b3 b4 b5 b6 b7
(f)
G0 G1 G2 G3 G4
(5) ビット列転置
(g)
G2 G4 G0 G1 G3

# LIST FOR IDS

REFERENCE WITH "-cb" ATTACHED TO THE NUMBER HAS BEEN CITED BEFORE, **REFERENCE WITHOUT THE SUFFIX WAS FIRST CITED IN THE ATTACHED OA**.

| SONY REF. | US SERIAL NO. | IDS TIMING |
|---|---|---|
| S00P1073US00 | 09/831071 | OA (JP) |

CORRESPONDING JAPANESE PATENT APPLICATION

JP 11 - 253660 | OA issued on: 2007/12/21 | [HQ-CASE]

| | PATENT DOCUMENT(S) | | | | ENGLISH EQUIVALENT |
|---|---|---|---|---|---|
| 1 | JPA | HEI | 10 - 283268 | ( JPA 1998 283268 ) | |
| 2 | JPA | HEI | 09 - 091344 | ( JPA 1997 091344 ) | |
| 3 | | | WO - 97/14144 | ( WO 97/14144 ) | |
| 4 | JPA | HEI | 09 - 326166 | ( JPA 1997 326166 ) | |
| 5 | JPA | HEI | 11 - 195269 | ( JPA 1999 195269 ) | |
| 6 | | | | | |
| 7 | | | | | |
| 8 | | | | | |
| 9 | | | | | |
| 10 | | | | | |
| 11 | | | | | |
| 12 | | | | | |
| 13 | | | | | |
| 14 | | | | | |
| 15 | | | | | |

| | NON-PATENT DOCUMENT(S) | ENGLISH |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

**特開平11－195269**

(43)公開日　平成11年(1999)７月21日

| (51)Int.Cl.[6] | 識別記号 | ＦＩ | |
|---|---|---|---|
| Ｇ１１Ｂ　20/10 | | Ｇ１１Ｂ　20/10 | Ｈ |
| Ｇ０９Ｃ　1/00 | ６１０ | Ｇ０９Ｃ　1/00 | ６１０Ｚ |
| | ６６０ | | ６６０Ｄ |
| Ｈ０４Ｌ　9/16 | | Ｈ０４Ｌ　9/00 | ６４３ |
| // Ｇ０６Ｆ　17/60 | | Ｇ０６Ｆ　15/21 | ３４０Ｚ |

審査請求　未請求　請求項の数９　ＦＤ　（全９頁）

(21)出願番号　特願平9－369395

(22)出願日　平成９年(1997)12月26日

(71)出願人　000004329
日本ビクター株式会社
神奈川県横浜市神奈川区守屋町３丁目12番地

(72)発明者　平田　渥美
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内

(72)発明者　町田　豊隆
千葉県柏市篠籠田1135－１　サルビア703

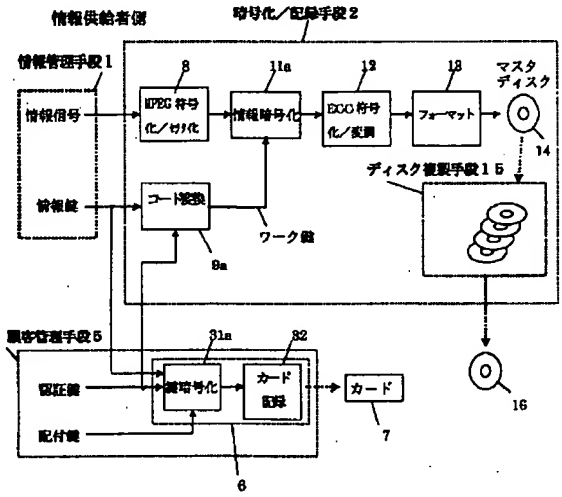
(72)発明者　廣田　昭
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内

(54)【発明の名称】　情報暗号化方法、情報復号方法、情報暗号化装置、情報復号装置及び情報記録媒体

(57)【要約】

【課題】　比較的簡単で安価に暗号化及び復号が可能で、しかも復号鍵の推定が困難な情報暗号化方法がなかった。

【解決手段】　情報管理手段１は、デジタル情報に固有の情報鍵コードと情報信号とを蓄積している。また、顧客管理手段５は、顧客固有の認証鍵と再生装置固有の配付鍵を蓄積している。そして、コード変換手段９ａにより情報鍵コードをコード変換してワーク鍵コードを生成する。さらに、情報暗号化手段１１ａでは、コード変換手段９ａより出力されるワーク鍵コードとセクタ番号とから暗号化鍵コードを生成し、この暗号化鍵コードを使用してセクタ化されたデジタル情報データを暗号化する。



【特許請求の範囲】
【請求項１】デジタル情報データを複数のセクタに分割してセクタの序列を示すセクタ番号と共に情報記録媒体に記録する際に前記デジタル情報データを暗号化する情報暗号化方法において、
前記デジタル情報に固有の情報鍵コードをコード変換してワーク鍵コードを生成し、
このワーク鍵コードと前記セクタ番号とから暗号化鍵コードを生成し、
この暗号化鍵コードを使用してセクタ化された前記デジタル情報データを暗号化することを特徴とする情報暗号化方法。
【請求項２】複数のセクタに分割されて暗号化されたデジタル情報データがセクタの序列を示すセクタ番号と共に記録されている記録媒体の前記デジタル情報データを復号する情報復号方法において、
前記記録媒体以外から供給される暗号化された前記デジタル情報に固有の情報鍵コードを復号し、
この情報鍵コードをコード変換してワーク鍵コードを生成し、
このワーク鍵コードと前記記録媒体に記録されている前記セクタ番号とから復号化鍵コードを生成し、
この復号化鍵コードを使用して前記記録媒体を再生して得られる暗号化されたデジタル情報を復号することを特徴とする情報復号方法。
【請求項３】前記ワーク鍵コードは、
情報鍵コードを等ビット数の複数部分ビット列に分割し、この部分ビット列から選択される任意の一つの部分ビット列を、それぞれ他の各部分ビット列に排他的論理加算してから結合して第一のビット列を生成し、
前記第一のビット列に前記情報鍵コードと同じビット数の第二のビット列を排他的論理加算して第三のビット列を生成し、
前記第三のビット列を等ビット数の複数の部分ビット列に分割し、この各部分ビット列内で所定のビット数だけ右又は左にローテートした後、結合して第四のビット列を生成し、
前記第四のビット列を複数の部分ビット列に分割し、各部分ビット列の配列順序を変更して生成されることを特徴とする請求項１記載の情報暗号化方法又は請求項２記載の情報復号方法。
【請求項４】前記暗号化鍵コード又は前記復号化鍵コードは、前記ワーク鍵コードを前記セクタ番号で除算した余り値を使用して発生した擬似ランダムコード列であることを特徴とする請求項１記載の情報暗号化方法又は請求項２記載の情報復号方法。
【請求項５】デジタル情報データを複数のセクタに分割してセクタの序列を示すセクタ番号と共に情報記録媒体に記録する際に前記デジタル情報データを暗号化する情報暗号化装置において、
前記デジタル情報に固有の情報鍵コードをコード変換してワーク鍵コードを生するコード変換手段と、
このコード変換手段より出力されるワーク鍵コードと前記セクタ番号とから暗号化鍵コードを生成し、この暗号化鍵コードを使用してセクタ化された前記デジタル情報データを暗号化する情報暗号化手段とを有することを特徴とする情報暗号化装置。
【請求項６】複数のセクタに分割されて暗号化されたデジタル情報データがセクタの序列を示すセクタ番号と共に記録されている記録媒体の前記デジタル情報データを復号する情報復号装置において、
前記記録媒体以外から供給される暗号化された前記デジタル情報に固有の情報鍵コードを復号する鍵復号手段と、
この鍵復号手段にて復号された情報鍵コードをコード変換してワーク鍵コードを生成するコード変換手段と、
このコード変換手段にて生成されたワーク鍵コードと前記記録媒体に記録されている前記セクタ番号とから復号化鍵コードを生成し、この復号化鍵コードを使用して前記記録媒体を再生して得られる暗号化されたデジタル情報を復号する情報復号化手段とを有することを特徴とする情報復号装置。
【請求項７】前記コード変換手段は、
情報鍵コードを等ビット数の複数部分ビット列に分割し、この部分ビット列から選択される任意の一つの部分ビット列を、それぞれ他の各部分ビット列に排他的論理加算してから結合して第一のビット列を生成するビット列分割／加算手段と、
前記第一のビット列に前記情報鍵コードと同じビット数の第二のビット列を排他的論理加算して第三のビット列を生成する加算手段と、
前記第三のビット列を等ビット数の複数の部分ビット列に分割し、この各部分ビット列内で所定のビット数だけ右又は左にローテートした後、結合して第四のビット列を生成するビットローテーション手段と、
前記第四のビット列を複数の部分ビット列に分割し、各部分ビット列の配列順序を変更してワーク鍵コード得ることを特徴とする請求項５記載の情報暗号化装置又は請求項６記載の情報復号装置。
【請求項８】前記暗号化鍵コード又は前記復号化鍵コードは、前記ワーク鍵コードを前記セクタ番号で除算した余り値を使用して発生した擬似ランダムコード列であることを特徴とする請求項５記載の情報暗号化装置又は請求項６記載の情報復号装置。
【請求項９】複数のセクタに分割されたデジタル情報データがセクタの序列を示すセクタ番号と共に記録されている情報記録媒体であって、
前記デジタル情報データは、前記デジタル情報に固有の情報鍵コードをコード変換したワーク鍵コードと前記セクタ番号とから生成される暗号化鍵コードを使用して暗

号化されていることを特徴とする情報記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報の暗号化／復号方法に係り、特に、映像信号、音声信号、データ信号等の情報をセクタ化して、ディスク等の情報記録媒体に記録／再生を行う場合に用いて好適な情報暗号化方法、情報復号方法、情報暗号化装置、情報復号装置及び情報記録媒体に関するものである。

【０００２】

【従来の技術】従来より、所定の記録媒体に情報を暗号化して記録する場合、所定の暗号化鍵を用いて情報を暗号化して所定の記録媒体に記録すると同時に、暗号化された情報を復号するための復号鍵（あるいは復号鍵に対応する情報）を、同一記録媒体に記録している。この場合、復号鍵（あるいは復号鍵に対応する情報）は、記録媒体の所定の連続した領域に連続して記録、あるいは、連続しない複数の領域に分散して記録している。

【０００３】復号は、記録媒体から再生して得た復号鍵、あるいは復号鍵に対応する情報を基に生成した復号鍵を用いて、同じ記録媒体から再生される暗号化された情報を復号していた。

【０００４】また、暗号化は、少なくとも一つの情報については一つの暗号鍵を用いて暗号化している。例えば、60分間長の映画の情報を暗号化する場合、60分間全編に亙って同一の暗号鍵を用いて暗号化していた。

【０００５】

【発明が解決しようとする課題】従来は、暗号化された情報と、その暗号化された情報を復号するために用いる復号鍵（あるいは復号鍵に対応する情報）とが、同一の記録媒体に記録されており、また一つの情報全体に亙って同一暗号鍵を用いて暗号化しているため、復号鍵を推定され易いという課題があった。また、情報記録媒体内に、復号鍵（あるいは復号鍵に対応する情報）を記録しているので、情報記録媒体内にそのための領域を確保する必要があり、その分、本来の情報を記録する領域が減少していた。

【０００６】なお、比較的簡単で且つ効果的な暗号化／復号化方法として、共通鍵方式によるPN加算方式がある。この方式は、擬似ランダム加算方式とも呼ばれ、M系列符号発生器を利用して情報を暗号化するものである。しかし、この方式でも、内容に一定の規則性がある複数個の復号鍵を準備し、それらを一つづつ用いて、暗号化された情報の復号を試み、個々の復号結果と、復号鍵間の規則性との相関を解析することによって、その暗号化された情報に用いられた暗号鍵及びその復号鍵を推定することが比較的容易に可能である。したがって、暗号化された情報を不正に解読される危険性があった。

【０００７】また、これらの問題を解決する方法として、例えば、ブロック暗号化方式、公開鍵方式等種々提案されているが、いずれも複雑で復号処理に時間が掛かるので、映画や音楽などのリアルタイムで再生する必要のある情報の暗号化処理には不向きであったり、高価な装置が必要になったりする等の問題があった。

【０００８】そこで本発明は、比較的簡単で安価に暗号化及び復号が可能で、しかも復号鍵の推定が困難な情報暗号化方法、情報復号化方法、情報暗号化装置、情報復号化装置及び情報記録媒体を提供することを目的とする。

【０００９】

【課題を解決するための手段】上記目的を達成するための手段として、以下の情報暗号化方法、情報復号化方法、情報暗号化装置、情報復号化装置及び情報記録媒体を提供する。

【００１０】１．デジタル情報データを複数のセクタに分割してセクタの序列を示すセクタ番号と共に情報記録媒体に記録する際に前記デジタル情報データを暗号化する情報暗号化方法において、前記デジタル情報に固有の情報鍵コードをコード変換してワーク鍵コードを生成し、このワーク鍵コードと前記セクタ番号とから暗号化鍵コードを生成し、この暗号化鍵コードを使用してセクタ化された前記デジタル情報データを暗号化することを特徴とする情報暗号化方法。

【００１１】２．複数のセクタに分割されて暗号化されたデジタル情報データがセクタの序列を示すセクタ番号と共に記録されている記録媒体の前記デジタル情報データを復号する情報復号方法において、前記記録媒体以外から供給される暗号化された前記デジタル情報に固有の情報鍵コードを復号し、この情報鍵コードをコード変換してワーク鍵コードを生成し、このワーク鍵コードと前記記録媒体に記録されている前記セクタ番号とから復号化鍵コードを生成し、この復号化鍵コードを使用して前記記録媒体を再生して得られる暗号化されたデジタル情報を復号することを特徴とする情報復号方法。

【００１２】３．前記ワーク鍵コードは、情報鍵コードを等ビット数の複数部分ビット列に分割し、この部分ビット列から選択される任意の一つの部分ビット列を、それぞれ他の各部分ビット列に排他的論理加算してから結合して第一のビット列を生成し、前記第一のビット列に前記情報鍵コードと同じビット数の第二のビット列を排他的論理加算して第三のビット列を生成し、前記第三のビット列を等ビット数の複数の部分ビット列に分割し、この各部分ビット列内で所定のビット数だけ右又は左にローテートした後、結合して第四のビット列を生成し、前記第四のビット列を複数の部分ビット列に分割し、各部分ビット列の配列順序を変更して生成されることを特徴とする上記１記載の情報暗号化方法又は上記２記載の情報復号方法。

【００１３】４．前記暗号化鍵コード又は前記復号化鍵コードは、前記ワーク鍵コードを前記セクタ番号で除算

した余り値を使用して発生した擬似ランダムコード列であることを特徴とする上記１記載の情報暗号化方法又は上記２記載の情報復号方法。

【００１４】５．デジタル情報データを複数のセクタに分割してセクタの序列を示すセクタ番号と共に情報記録媒体に記録する際に前記デジタル情報データを暗号化する情報暗号化装置において、前記デジタル情報に固有の情報鍵コードをコード変換してワーク鍵コードを生するコード変換手段と、このコード変換手段より出力されるワーク鍵コードと前記セクタ番号とから暗号化鍵コードを生成し、この暗号化鍵コードを使用してセクタ化された前記デジタル情報データを暗号化する情報暗号化手段とを有することを特徴とする情報暗号化装置。

【００１５】６．複数のセクタに分割されて暗号化されたデジタル情報データがセクタの序列を示すセクタ番号と共に記録されている記録媒体の前記デジタル情報データを復号する情報復号装置において、前記記録媒体以外から供給される暗号化された前記デジタル情報に固有の情報鍵コードを復号する鍵復号手段と、この鍵復号手段にて復号された情報鍵コードをコード変換してワーク鍵コードを生成するコード変換手段と、このコード変換手段にて生成されたワーク鍵コードと前記記録媒体に記録されている前記セクタ番号とから復号化鍵コードを生成し、この復号化鍵コードを使用して前記記録媒体を再生して得られる暗号化されたデジタル情報を復号する情報復号化手段とを有することを特徴とする情報復号装置。

【００１６】７．前記コード変換手段は、情報鍵コードを等ビット数の複数部分ビット列に分割し、この部分ビット列から選択される任意の一つの部分ビット列を、それぞれ他の各部分ビット列に排他的論理加算してから結合して第一のビット列を生成するビット列分割／加算手段と、前記第一のビット列に前記情報鍵コードと同じビット数の第二のビット列を排他的論理加算して第三のビット列を生成する加算手段と、前記第三のビット列を等ビット数の複数の部分ビット列に分割し、この各部分ビット列内で所定のビット数だけ右又は左にローテートした後、結合して第四のビット列を生成するビットローテーション手段と、前記第四のビット列を複数の部分ビット列に分割し、各部分ビット列の配列順序を変更してワーク鍵コード得ることを特徴とする上記５記載の情報暗号化装置又は上記６記載の情報復号装置。

【００１７】８．前記暗号化鍵コード又は前記復号化鍵コードは、前記ワーク鍵コードを前記セクタ番号で除算した余り値を使用して発生した擬似ランダムコード列であることを特徴とする上記５記載の情報暗号化装置又は上記６記載の情報復号装置。

【００１８】９．複数のセクタに分割されたデジタル情報データがセクタの序列を示すセクタ番号と共に記録されている情報記録媒体であって、前記デジタル情報データは、前記デジタル情報に固有の情報鍵コードをコード変換したワーク鍵コードと前記セクタ番号とから生成される暗号化鍵コードを使用して暗号化されていることを特徴とする情報記録媒体。

【００１９】

【発明の実施の形態】本発明の情報暗号化方法、情報復号化方法、情報暗号化装置、情報復号化装置及び情報記録媒体の詳細な説明をするのに先だって、先ず本発明の利用分野である情報供給システムの概要について図１を用いて説明する。

【００２０】同図において、情報の供給者は、記録媒体３に記録して販売等に供する情報（コンテンツ）の管理や情報に固有の情報鍵の生成管理等を行う情報管理手段１と、顧客情報の管理、配付鍵や認証鍵の生成管理、課金管理等を行う顧客管理手段５とを有している。

【００２１】そして、所定の情報を所定の顧客に供給するに当たっては、まず、情報供給者は、暗号化／記録手段２において、顧客が所望する情報を、その情報に固有の情報鍵及び顧客に情報の取得を認可する認証鍵を用いて暗号化し、所定の情報記録媒体３に記録して顧客に供給する一方で、暗号化された情報を復号するために用いる復号鍵を生成するための情報として、情報鍵、認証鍵等（あるいは、それらに対応した情報等）を配付鍵を用いて暗号化し、カード発行手段６によってカード７に記録して、顧客に配付する。　顧客は受け取った情報記録媒体３及びカード７を再生／復号化手段４に装着して、所定の情報を取得する。なお、認証鍵は、顧客あるいは顧客が属するグループ等に固有の予め付与した情報であり、また、配付鍵は顧客が使用する情報再生／復号装置に固有の予め付与した情報である。

【００２２】このような情報供給システムにおいて本発明は、この暗号化および復号化に関して新たな提案を行うものである。すなわち、本発明は、デジタル情報を複数のセクタに分割し、各セクタに付与したセクタ番号及び情報に固有の情報鍵を基に生成した暗号鍵を用いて、各セクタ毎に情報を暗号化し、その暗号化したデジタル情報データを記録媒体に記録するものである。

【００２３】ここで、セクタ番号は各セクタに固有の番号であるため、各セクタはそれぞれセクタに固有の暗号鍵を用いて暗号化されることになる。すなわち、情報は、頻繁に（下記に詳述する実施例では約0.003秒間隔で）更新される暗号鍵を用いて暗号化される。この様に短い間隔で暗号鍵が更新されるため、暗号化された情報から、それに用いられた暗号鍵及びその復号鍵を推定することは極めて困難となる。

【００２４】また、暗号化及び復号化に当たって、情報鍵コードを別のコードに変換し、その変換されたワーク鍵コードを用いて暗号鍵及び復号鍵を生成している。これにより、互いに規則性のある複数個の情報鍵を準備して復号鍵の推定を試みようとしても、このコード変換によって、規則性が崩れるため復号鍵の推定が困難とな

る。

【００２５】以下、本発明の情報暗号化方法、情報復号化方法、情報暗号化装置、情報復号化装置及び情報記録媒体の一実施例として、暗号化された情報を記録する記録媒体としてＤＶＤ(Digital Versatile Disk)を用いた場合について説明する。なお、本発明で使用する情報記録媒体としては、ＤＶＤに限らず、他の磁気テープ、磁気ディスク等も有効である。

【００２６】

【実施例】図２は、本発明の暗号化装置でる情報供給側の構成例を示すブロック図である。同図において、情報管理手段１は、販売等に供する情報（映像情報、音声情報、データ情報等のコンテンツ情報、以下コンテンツ情報ともいう）を在庫として保有するとともにそれを管理し、必要に応じて情報信号を暗号化して記録媒体に記録するために、暗号化／記録手段２に供給するものである。また、情報信号を暗号化／記録手段２に供給する際には、そのコンテンツ情報に固有の情報である情報鍵コードを、暗号化／記録手段２及び顧客管理手段５に供給する。

【００２７】顧客管理手段５は、配付鍵、認証鍵等の管理を行い、コンテンツ情報を顧客に供給する際に、認証鍵コードを暗号化／記録手段２に供給する。　また、配付鍵コードを用いて、情報鍵コード及び認証鍵コードを暗号化し、カード記録手段３２に出力してカード状情報記録媒体（以下、カードと記す）７に記録して、顧客（ユーザ、情報利用者）に配付する。なお、認証鍵は、ユーザあるいはユーザが属するグループ等を識別するための固有の情報（例えば会員番号や顧客管理番号）であり、また、配付鍵はユーザが使用する情報再生／復号手段４を識別するための固有の情報（例えば装置の製造番号等の識別番号）である。

【００２８】情報管理手段１から暗号化／記録手段２に供給された情報信号は、まず、ＭＰＥＧ符号化／セクタ化手段８に入力される。ＭＰＥＧ符号化／セクタ化手段８は、入力された情報信号をＭＰＥＧ方式による圧縮符号化を行ってデジタル情報データを生成し、更に、このデジタル情報データを2048バイトから成る複数のセクタに分割する。

【００２９】その後、ＤＶＤフォーマットに合わせるために、各セクタにセクタ管理情報、セクタ番号等を付加して、2064バイトで構成されるデータセクタを構築し、順次、暗号化手段１１ａに供給する。

【００３０】このＭＰＥＧ符号化／セクタ化手段８で構築されるデータセクタの構造を図４に示す。図４（b）に示す１データセクタは、IDデータ(4バイト)、IDデータのエラー検出符号であるIED(2バイト)、メインデータ(2048バイト)及びメインデータのエラー検出符号であるEDC(4バイト)で構成されている。更に、このIDデータは図４（a）に示すように、セクタ情報データ(1バイト)とセクタ番号(3バイト)とで構成される。なお、セクタ化されたデジタル情報データは、上記のメインデータ領域に収納される。また、セクタ番号は、各データセクタの序列を示し、通常は最初のセクタからの通し番号である。

【００３１】また、情報管理手段１から暗号化／記録手段２に供給された情報鍵コードは、コード変換器９ａに入力される。また、顧客管理手段５から暗号化／記録手段２に供給された認証鍵コードも、コード変換器９ａに入力される。そして、コード変換器９ａは、入力された情報鍵コードと認証鍵コードとの間で後述する所定の演算及びコード変換処理を行ない、その結果得たワーク鍵コードを暗号手段１１ａに供給する。

【００３２】ここでは、情報鍵コードを暗号鍵生成要素の一つとして使用しているが、情報管理手段１から供給された情報鍵コードを、別のコードに変換することによって、暗号鍵および復号鍵の秘匿性を高めている。そして、図６にコード変換器9aの構成例を示し、図７にその演算及びコード変換処理の手順を示す。情報鍵コードは、下述の手順でコード変換されてワーク鍵コードとして出力される。

【００３３】入力される情報鍵コードは、ビット列分割／加算器２７に供給される。ビット列分割／加算器２７は、供給される入力コード（情報鍵コード）を任意の等ビット長からなる複数の部分ビット列D0, D1, …, D9に分割する（図７(a)）。そして、一つの部分ビット列（実施例ではD4であるが、これに限らない）を、残りの各部分ビット列に、個別に排他的論理加算して新たな部分ビット列（第一のビット列）E0, E1, …, E9を得る。この時、Ｄ４同士の排他的論理和は採らずにE4 = D4とする。そして、これらの部分ビット列E0, E1, …, E9を結合して新たなビット列を得て、加算器３０に出力する（図７(b)）。

【００３４】加算器３０は、ビット列分割／加算器２７から供給される新たなビット列に対して、顧客管理手段５から供給される情報鍵コードと等ビット数の認証鍵コード（図７(c)，第二のビット列）を排他的論理加算し、得られたビット列を任意の等ビット長の複数の部分ビット列（第三のビット列）F0, F1, …, F4に分割してビットローテーション器２８に出力する（図７(d)）。

【００３５】ビットローテーション器２８は、供給される部分ビット列F0, F1, …, F4を分割された各部分ビット列単位（F0内、F1内、…）で、所定のビット数だけ右にローテートし（図７(e)）、部分ビット列G0, G1, …, G4（第四のビット列）を得る（図７(f)）。この部分ビット列G0, G1, …, G4は、ビット列転置器２９に供給され、部分ビット列G0, G1, …, G4の配列順序を任意に変更する。そして、その結果得たビット列をワーク鍵コードとして情報暗号化手段１１ａに出力する（図７(g)）。

【００３６】以上説明したコード変換器９ａは、入力情

報鍵コードを一意のワーク鍵コードに変換し、入力情報鍵コードが規則的に変化しても、それに対応してワーク鍵コードはランダムに変化すると言う特徴を有して居るので、この様なワーク鍵コードを用いて暗号化された情報から、それを復号するための復号鍵を推測することは極めて困難である。

【００３７】なお、上記した各部分ビット列のビット長や分割数などは任意であるが、後述する再生／復号手段４で使用するコード変換手段９ｂと同じビット長及び分割数の部分ビット列とする必要がある。

【００３８】情報暗号化手段１１ａは、コード変換器９ａから供給されたワーク鍵コードに基づいて、ＭＰＥＧ符号化／セクタ化手段８から供給されたセクタデータを暗号化し、暗号化されたセクタデータをＥＣＣ符号化／変調手段１２に供給する。

【００３９】ここで、情報暗号化手段１１ａの構成例を図５に示し、図４を参照しながらその動作について説明する。同図において、セクタデータは、入力ビット列として信号分割器２２及びセクタ解読器２３に入力される。また、ワーク鍵コードは除算器２１に入力される。

【００４０】セクタ解読器２３は、セクタデータ内のIDデータを検出解読して、入力ビット列がメインデータ領域期間中である場合には、分割制御信号（図４(d)）を信号分割器22に供給する。また、セクタ番号を抽出して、除算器２１に出力する。さらに、各セクタの開始時点（メインデータ領域期間となる前）に、初期化制御信号（図４(c)）をM列符号発生器２４に供給する。

【００４１】信号分割器２２は、セクタ解読器23から供給される分割制御信号に応じて、セクタデータ内のメインデータを加算器２６に供給すると共に、それ以外のデータを信号結合器２５に供給する。

【００４２】一方、除算器２１は、セクタ解読器２３から供給されるセクタ番号でワーク鍵コードを除算し、その結果得た余り値を初期値としてM系列符号発生器２４に供給する。M系列符号発生器２４は、セクタ解読器２３から初期化制御信号が供給される度に、除算器２１から供給される余り値を初期値として、疑似ランダムコード列（暗号化鍵コード）を発生し、加算器２６に出力する。

【００４３】加算器２６は、信号分割器２２から供給されるメインデータに、M系列符号発生器２４から供給された疑似ランダムコードを排他論理加算することによってこれらを暗号化し、暗号化されたメインデータを信号結合器２５に供給する。信号結合器２５は、信号分割器２２から供給されるIDデータ、IEDデータ及び著作権管理情報データと、加算器２６から供給される暗号化されたメインデータとを結合して、暗号化されたセクタデータ（図４(e)）を出力する。

【００４４】ここで、IDデータ内のセクタ番号は、既述のごとく各セクタに固有の値である。したがって、M系列符号発生器２４は、各セクタ毎に、そのセクタに固有の値を初期値として疑似ランダムコード列を発生することになる。したがって、各セクタは、それぞれ異なるコード列で暗号化される。

【００４５】また、１セクタは、既述のごとく2064バイト長であり、これは実時間再生で0.003秒間程度に相当する。すなわち、暗号化パターンが約0.003秒間隔で次々と変わることになる。したがって、情報記録媒体に記録された暗号化されたデータを再生して、そのデータパターンを解析して暗号鍵／復号鍵の解読を試みても、この様な短期間に解読することは困難である。

【００４６】このようにして、情報暗号化手段１１ａは、各データセクタごとに暗号化されたセクタデータ列をＥＣ符号化／変調器１２に出力する。そして、情報暗号化器１１ａから出力された暗号化されたセクタデータ列は、公知のＥＣ符号化／変調器１２及び公知のフォーマット手段１３により所定の処理を施されて、マスタディスク１４に記録される。さらに、このマスタディスク１４を基に、公知ディスク複製手段１５を用いて、再生用ディスク１６を複製してユーザに供給する。なお、多くの再生用ディスク１６を必要としない場合には、マスタディスク１４をユーザ供給用として使用しても良い。

【００４７】さらに、情報提供者は、鍵暗号化手段３１ａにより、前述の情報鍵コード及び認証鍵コードを配付鍵コードを用いてそれぞれ暗号化し、カード記録手段３２に供給してカード７に記録する。そして、このようにして配付鍵コードで暗号化された情報鍵コード及び認証鍵コードを記録したカード７をユーザに配付する。なお、鍵暗号化手段３１ａでの暗号化の手法やカード記録手段３２及びカード７は特定のものである必要はなく、種々のものを使用することができる。

【００４８】図３は、ユーザ側（情報利用者側）の構成例を示す図である。ユーザは、暗号化されたコンテンツ情報が記録された再生用ディスク（情報記録媒体）１６と、暗号化された情報を復号するために必要な情報が記録されたカード７とを再生／復号手段４に装着して、暗号化されたコンテンツ情報を再生復号する。

【００４９】同図に示す再生／復号手段４は、再生用ディスク１６からデータを読み取ってデジタルデータを出力する公知の情報再生手段１７と、データセクタに含まれるＩＥＤやＥＤＣを使用してエラー訂正をすると共に情報の復調を行う公知の復調／エラー訂正手段１８と、情報復号化手段１１ｂと、カード解読手段１９と、配付鍵格納手段３３と、鍵復号手段３１ｂと、コード変換器９ｂ及び公知のセクタ分解／ＭＰＥＧ復号手段２０で構成されている。なお、コード変換器９ｂ及び情報復号化手段１１ｂは、それぞれ、既述の暗号化／記録手段２における、コード変換器９ａ及び情報暗号化手段１１ａと全く同一構成であり、同一動作及び同一機能を有している。

【００５０】再生手段１７は、再生用ディスク１６から再生して得た再生情報を、復調／エラー訂正手段１８に供給する。復調／エラー訂正手段１８は、再生情報を復調してエラー訂正処理し、暗号化されたセクタデータを得て情報復号化手段１１ｂに供給する。

【００５１】一方、カード解読手段１９は、カード7に記録されている暗号化された情報鍵コード及び暗号化された認証鍵コードを読み出し、これらを鍵復号手段３１ｂに供給する。

【００５２】鍵復号手段３１ｂは、配付鍵格納手段３３に格納されている配付鍵を用いて、暗号化されている情報鍵コードと認証鍵コードをそれぞれ復号して、情報鍵コードと認証鍵コードとをコード変換器９ｂに出力する。なお、配付鍵格納手段３３に格納されている配付鍵は、再生／復号手段４に予め付与された装置の識別番号（例えば製造番号等）であり、顧客管理手段５に格納されている配付鍵と同一のものが使用される。なお、カード解読手段１９及び鍵復号手段３１ｂは種々のもの及び方法を使用することができる。

【００５３】コード変換器９ｂの構成例を図６に示す。これは、既述の暗号化／記録手段２で用いたコード変換器９ａと同一構成であるので、その動作の詳細な説明は省略する。そして、鍵復号手段３１ｂから供給される認証鍵コードを用いて、同じく鍵復号手段３１ｂから供給される情報鍵コードをワーク鍵コードに変換し、これを情報復号手段１１ｂに出力する。

【００５４】図５に情報復号化手段１１ｂの構成例を示す。これは既述の情報暗号化手段１１ａと同一構成であり、その詳細な説明は省略するが、M系列符号発生手段２４から出力される擬似ランダムコード列は復号鍵コードとして使用される。したがって、情報暗号化手段１１ａの場合は、入力ビット列として暗号化するべきセクタデータが入力され、出力ビット列として暗号化されたセクタデータが出力されるが、情報復号化手段１１ｂでは、入力ビット列として暗号化されたセクタデータが入力され、出力ビット列として暗号化されたセクタデータを復号したセクタデータが出力される。ここで、ワーク鍵コードは、暗号化の場合と復号化の場合とで、同一コードある。したがって、暗号化されたセクタデータは、正確に元のセクタデータに復号される。

【００５５】そして、復号されたセクタは、セクタ分離／ＭＰＥＧ復号手段２０に出力され、元の情報信号にＭＰＥＧ復号されて出力される。

【００５６】

【発明の効果】本発明の情報暗号化方法、情報復号方法、情報暗号化装置及び情報復号装置情報記録媒体は、簡単な手段で強力な暗号化を行うことができる。

【００５７】そして、本発明の情報記録媒体は、暗号鍵／復号鍵に関する情報を記録する必要がないので、そのための記録領域を確保する必要なく、情報の記録領域を効率よく使用することができるという効果がある。

【図面の簡単な説明】

【図１】情報供給システムの一例を示す構成図である。

【図２】本発明の情報暗号化装置の一実施例を示す構成図である。

【図３】本発明の情報復号装置の一実施例を示す構成図である。

【図４】本発明の情報記録媒体に記録する情報のセクタ構造の例を示す図である。

【図５】情報暗号化手段及び情報復号手段の一実施例を示す構成図である。

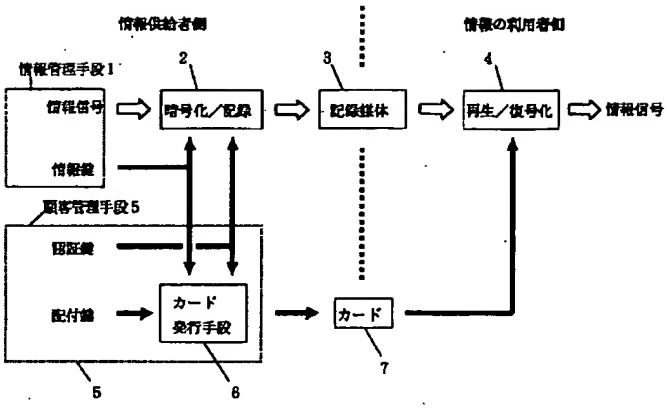
【図６】コード変換器の一実施例を示す構成図である。

【図７】コード変換器での動作の一例を説明するための図である。

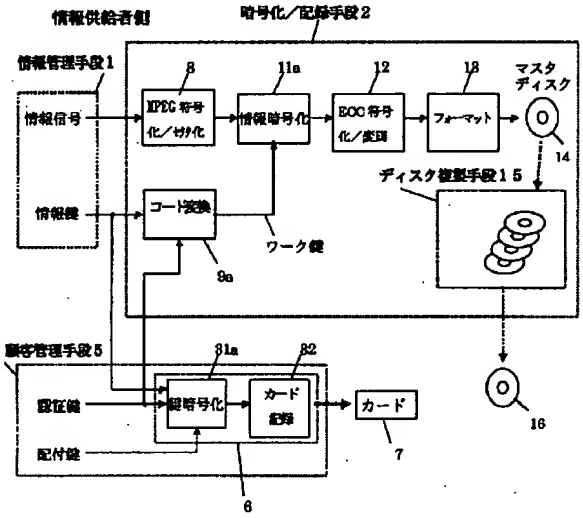
【符号の説明】

１　情報管理手段
２　暗号化／記録手段
３　情報記録媒体
４　再生／復号手段
５　顧客管理手段
６　カード発行手段
７　カード（カード状情報記録媒体）
８　ＭＰＥＧ符号化／セクタ化手段
９ａ，９ｂ　コード変換器（コード変換手段）
１１ａ　情報暗号化手段
１１ｂ　情報復号手段
１２　ＥＣＣ符号化／変調手段
１３　フォーマット手段
１４　マスタディスク
１５　ディスク複製手段
１６　再生用ディスク
１７　情報再生手段
１８　復調／エラー訂正手段
１９　カード解読手段
２０　セクタ分離／ＭＰＥＧ復号手段
２１　除算器
２２　信号分割手段
２３　セクタ解読手段
２４　M系列符号発生器
２５　信号結合手段
２６　加算器
２７　ビット列分割／加算器
２８　ビットローテーション手段
２９　ビット列転置手段
３０　加算器
３１ａ　鍵暗号化手段
３１ｂ　鍵復号手段
３２　カード記録手段
３３　配付鍵格納手段

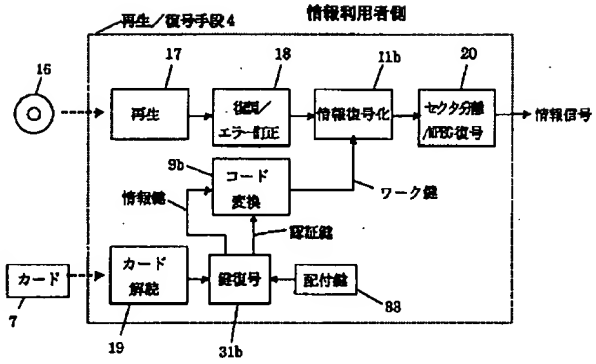
【図１】


情報供給者側
情報の利用者側
情報管理手段1
2
3
4
情報信号
暗号化／記録
記録媒体
再生／復号化
情報信号
情報鍵
顧客管理手段5
認証鍵
配付鍵
カード発行手段
カード
5
6
7

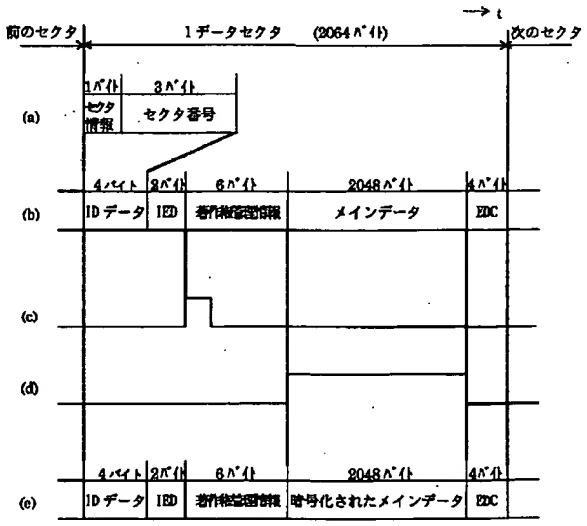
【図２】


情報供給者側
暗号化／記録手段2
情報管理手段1
8
11a
12
13
マスタディスク
情報信号
MPEG符号化／サブ化
情報暗号化
ECC符号化／変調
フォーマット
14
情報鍵
コード変換
ワーク鍵
9a
ディスク複製手段15
顧客管理手段5
31a
32
認証鍵
鍵暗号化
カード記録
カード
配付鍵
7
6
16

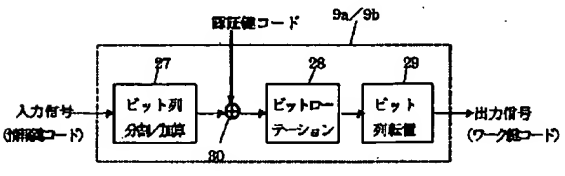
【図３】


再生／復号手段4
情報利用者側
16
17
18
11b
20
再生
復調／エラー訂正
情報復号化
セクタ分離／MPEG復号
情報信号
9b
コード変換
情報鍵
ワーク鍵
認証鍵
カード
カード解読
鍵復号
配付鍵
83
7
19
31b

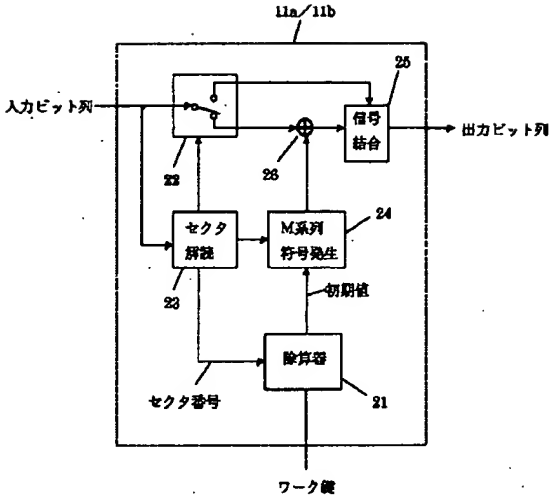
【図４】


t
前のセクタ
1データセクタ　(2064バイト)
次のセクタ
(a)
1バイト
セクタ情報
3バイト
セクタ番号
(b)
4バイト
2バイト
6バイト
2048バイト
4バイト
IDデータ
IED
著作権管理情報
メインデータ
EDC
(c)
(d)
(e)
暗号化されたメインデータ

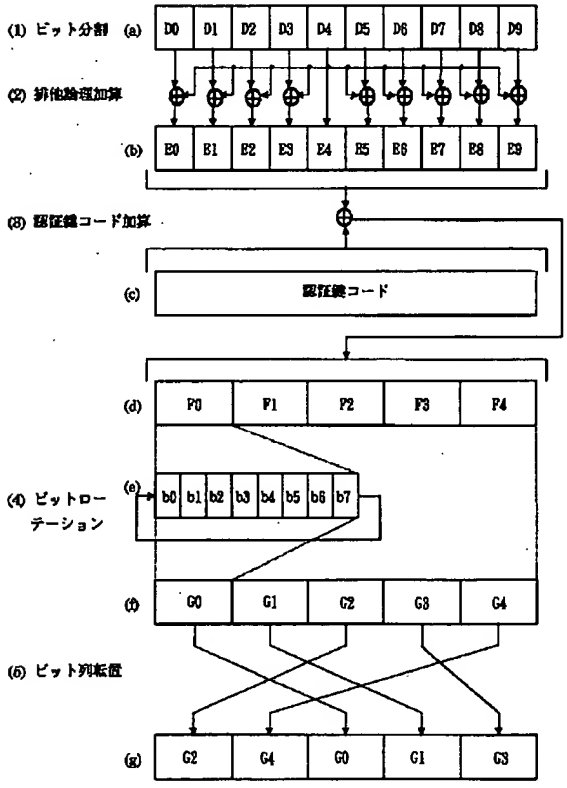
【図６】


認証鍵コード
9a／9b
27
28
29
入力信号（情報鍵コード）
ビット列分割／加算
ビットローテーション
ビット列転置
出力信号（ワーク鍵コード）
80

【図５】


11a/11b
25
入力ビット列
信号結合
出力ビット列
22
26
セクタ解読
M系列符号発生
24
23
初期値
除算器
セクタ番号
21
ワーク鍵

【図７】


(1) ビット分割
(a)
D0 D1 D2 D3 D4 D5 D6 D7 D8 D9
(2) 排他論理加算
(b)
E0 E1 E2 E3 E4 E5 E6 E7 E8 E9
(3) 認証鍵コード加算
(c)
認証鍵コード
(d)
F0 F1 F2 F3 F4
(4) ビットローテーション
(e)
b0 b1 b2 b3 b4 b5 b6 b7
(f)
G0 G1 G2 G3 G4
(5) ビット列転置
(g)
G2 G4 G0 G1 G3